目　录

第一章 整　　除

整除理论是初等数论的基础，它是对在小学就学过的整数的算术，主要是涉及除法运算的内容，作抽象的、系统的总结，看起来似乎很简单，但是它的内涵是十分重要而深刻的。本章的主要结果是数学中最重要、最基本、最著名的定理之一——算术基本定理，即每个大于1的正整数必可唯一地表为若干个素数的乘积，这一定理将在§6及§7讨论，分别给出了两个不同的证明。本章内容是围绕这一定理的讨论安排的。为了使讨论自然和方便，在§1中先概述了整数的加法、减法及乘法运算的概念与性质；整数的大小关系及其性质；特别是讨论了自然数的最重要的两个性质：自然数的归纳原理及由此推出的最小自然数原理，这是建立整除理论的基础，在本章及以后各章中经常要用到。在§3中，我们讨论建立整除理论的重要工具：带余数除法，并介绍了它的若干应用。在§2中，讨论整除的最简单的性质，这些性质实质上是不涉及加法、减法运算的；还引进了素数的概念，讨论了与素数有关的最简单性质。在§4中我们建立最大公约数理论，它是整除理论的核心内容，对此我们作了较全面的讨论。在第一部分，给出了不依赖于带余数除法的最大公约数及最小公倍数的性质；第二部分利用带余数除法建立了完整的最大公约数与最小公倍数理论，在这一部分中我们直接从定义出发，不需要利用最大公约数的明确表示式

$$(a,b)=ax+by,$$

但在证明中要用到较高的技巧；第三部分是在证明上式的基础上，利用它重新建立完整的最大公约数理论（不需要最小公倍数的概念与性质）。§5讨论所谓辗转相除法，即Euclid算法，它是

带余数除法的发展，利用它不仅可以证明上式成立，而且给出了寻找最大公约数(a,b)及x,y的有效算法。这一方法是十分有用的，在第七章将用它来建立连分数理论。最后，在§8中，我们引进一个在数学中十分有用的符号——实数x的最大整数部分$[x]$，并讨论它的性质。利用它我们给出了$n!$的素数乘积的表达式，它是除算术基本定理之外，另一个刻画自然数与素数之间关系的十分重要的关系式，我们将在第八章§2给出它的应用。

还应该指出的是，§6给出的算术基本定理的证明是利用§4建立的最大公约数理论，而§7给出的证明是直接的，它仅用到了最小自然数原理及大小关系的性质（实质上就是带余数除法），不需要最大公约数的任何知识。相反的，从算术基本定理出发也可以建立最大公约数与最小公倍数理论。

§1　自然数与整数

自然数，也叫**正整数**，就是大家所熟悉的

$$1,2,3,\cdots,n,n+1,\cdots. \tag{1}$$

我们以$\boldsymbol{N}$表由全体自然数(1)所组成的集合。**整数**就是指正整数、负整数及零，即

$$\cdots,-n-1,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots,n,n+1,\cdots. \tag{2}$$

我们以$\boldsymbol{Z}$表由全体整数(2)组成的集合。

在整数集合中可以作加法运算“+”及其逆运算减法运算“-”。加法运算满足以下性质：

(i)　**结合律**　$(a+b)+c=a+(b+c)$，　$a,b,c\in\boldsymbol{Z}$。

(ii)　**交换律**　$a+b=b+a$，　$a,b\in\boldsymbol{Z}$。

(iii)　**相消律**　$a+b=a+c\Longrightarrow b=c$，　$a,b,c\in\boldsymbol{Z}$。

(iv)　$a+0=a$，　$a\in\boldsymbol{Z}$。

(v)　对任意的$a,b\in\boldsymbol{Z}$，必有$x\in\boldsymbol{Z}$使得

$$a=b+x.$$

(v)就是减法运算的定义：$a-b=x$。

在整数集合中可以作乘法运算“·”，但不一定可作乘法的逆运算——除法运算。乘法运算满足以下性质：

(i) **结合律** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$， $a,b,c\in \boldsymbol{Z}$.

(ii) **交换律** $a\cdot b=b\cdot a$， $a,b\in \boldsymbol{Z}$。

(iii) **相消律** 若 $a\neq 0, a\cdot b=a\cdot c$，则 $b=c$， $a,b,c\in \boldsymbol{Z}$.

(iv) $0\cdot a=0$， $a\in \boldsymbol{Z}$。

(v) $1\cdot a=a$， $a\in \boldsymbol{Z}$.

(vi) **分配律** $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$， $a,b,c\in \boldsymbol{Z}$.

为简单起见，乘法 $a\cdot b$ 就记作 ab.

在整数中有大小（即顺序）关系，并用符号：$\leqslant, <, \geqslant$，及 $>$ 等来表示①．整数的顺序有以下性质：

(i) 对任意的 $a,b\in \boldsymbol{Z}$，关系

$$a=b,\quad a<b,\quad b<a$$

有且仅有一个成立.

(ii) **自反性** $a\leqslant a$， $a\in \boldsymbol{Z}$.

(iii) **反对称性** 对任意的 $a,b\in \boldsymbol{Z}$，若 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$.

(iv) **传递性** 对任意的 $a,b,c\in \boldsymbol{Z}$，若 $a\leqslant b$ 且 $b\leqslant c$，则 $a\leqslant c$，且等号仅当 $a=b, b=c$ 均成立时才成立.

(v) 对任意的 $a,b,c\in \boldsymbol{Z}$， $a+c\leqslant b+c \Longleftrightarrow a\leqslant b$.

(vi) 对任意的 $a,b,c\in \boldsymbol{N}$，若 $c=ab$，则 $a\leqslant c$，等号当且仅当 $b=1$ 时成立.

(vii) 对任意的 $a,b\in \boldsymbol{Z}$ 及 $c\in \boldsymbol{N}$, $ac\leqslant bc \Longleftrightarrow a\leqslant b$.

(viii) 对任意的 $a,b\in \boldsymbol{Z}$， $a\leqslant b \Longleftrightarrow -a\geqslant -b$.

在整数中还引入了绝对值的概念：

---

① $b\geqslant c$ 即 $c\leqslant b$. $a<b$ 表示 $a\leqslant b$ 且 $a\neq b$. $b>a$ 即 $a<b$.

$$|a|=\begin{cases} a, & a\in \boldsymbol{N}, \\ 0, & a=0, \\ -a, & -a\in \boldsymbol{N}. \end{cases}$$

它显然具有性质：

(i) $|ab|=|a||b|$，　$a,b\in \boldsymbol{Z}$.

(ii) $|a+b|\leqslant|a|+|b|$，　$a,b\in \boldsymbol{Z}$.

以上列举了一些熟知的有关整数的知识．对自然数来说它的最重要、最本质的性质是：

归纳原理　设 S 是 $\boldsymbol{N}$ 的一个子集，满足条件：(i) $1\in S$；(ii) 如果 $n\in S$，则 $n+1\in S$。那么，$S=\boldsymbol{N}$。

这原理是我们常用的数学归纳法的基础。

定理1（数学归纳法）　设 $P(n)$ 是关于自然数 n 的一种性质或命题。如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 由 $P(n)$ 成立必可推出 $P(n+1)$ 成立，

那么，$P(n)$ 对所有自然数 n 成立。

证　设使 $P(n)$ 成立的所有自然数 n 组成的集合是 S。S 是 $\boldsymbol{N}$ 的子集。由条件(i)知 $1\in S$；由条件(ii)知，若 $n\in S$，则 $n+1\in S$。所以由归纳原理知 $S=\boldsymbol{N}$。证毕。

由归纳原理还可推出两个在数学中，特别是初等数论中常用的自然数的重要性质。

定理2（最小自然数原理）　设 T 是 $\boldsymbol{N}$ 的一个非空子集．那么，必有 $t_0\in T$，使对任意的 $t\in T$ 有 $t_0\leqslant t$，即 t_0 是 T 中的最小自然数。

证　考虑由所有这样的自然数 s 组成的集合 S：对任意的 $t\in T$ 必有 $s\leqslant t$．由于 1 满足这样的条件，所以 $1\in S$，S 非空．此外，若 $t_1\in T$（因 T 非空所以必有 t_1），则 $t_1+1>t_1$，所以 $t_1+1\notin S$。由这两点及归纳原理就推出：必有 $s_0\in S$ 使得 $s_0+1\notin S$（为什么）．我们来证明必有 $s_0\in T$。因若不然，则对任意的 $t\in T$

必有 $t>s_0$，因而 $t\geqslant s_0+1$。这表明 $s_0+1\in S$，矛盾。取 $t_0=s_0$ 就证明了定理。

定理3（最大自然数原理） 设M是 $\boldsymbol{N}$ 的非空子集。若M有上界，即存在 $a\in\boldsymbol{N}$，使对任意的 $m\in M$ 有 $m\leqslant a$，那么，必有 $m_0\in M$，使对任意的 $m\in M$ 有 $m\leqslant m_0$，即 m_0 是M中的最大自然数。

证 考虑由所有这样的自然数 t 组成的集合T：对任意的 $m\in M$ 有 $m\leqslant t$。由条件知 $a\in T$，所以T非空。由定理2知，集合T中有最小自然数 t_0。我们来证明 $t_0\in M$。若不然，则对任意的 $m\in M$ 必有 $m<t_0$，因而 $m\leqslant t_0-1$。这样就推出 $t_0-1\in T$，但这和 t_0 的最小性矛盾。取 $m_0=t_0$ 就证明了定理。

最小自然数原理是我们常用的第二种数学归纳法的基础。

定理4（第二种数学归纳法） 设 $P(n)$是关于自然数 n 的一种性质或命题。如果

(i) 当 $n=1$时，$P(1)$成立；

(ii) 设 $n>1$。若对所有的自然数 $m<n$，$P(m)$成立，则必可推出 $P(n)$成立，

那么，$P(n)$对所有自然数 n 成立。

证 用反证法。若定理不成立，设T是使 $P(n)$不成立的所有自然数组成的集合，T非空。由定理2知集合T必有最小自然数 t_0。由于 $P(1)$成立，所以 $t_0>1$。由条件(ii)(取 $n=t_0$)知，必有自然数 $m<t_0$ 使 $P(m)$不成立。由T的定义知 $m\in T$，但这和t_0的最小性矛盾。证毕。

有的读者可能会感到奇怪，为什么这些"显然"正确的事实，在这里作为重要的定理列出并加以证明，认为这样是没有必要的。关于这一点我们不想在此作进一步的讨论，也不要求读者去深入探究，因为这涉及到数学的一些基本问题。有兴趣的读者，特别是准备当教师的读者，为了对"自然数"有更正确的认识，可阅读附录一，那里介绍了自然数的公理化定义，并初步讨

论了上面所提的问题（亦见附录一的习题）。

以上列出的性质和定理是初等数论的基础，读者必须熟练掌握。

此外，在初等数论中还经常用到的一个工具是：

鸽巢原理① 设 n 是一个自然数。现有 n 个盒子和 $n+1$ 个物体。无论怎样把这 $n+1$ 个物体放入这 n 个盒子中，一定有一个盒子中被放了两个或两个以上的物体。

证 用反证法。假设结论不成立，即每个盒子中至多有一个物体，那么，这 n 个盒子中总共有的物体个数 $\leqslant n$。这和有 $n+1$ 个物体放到了这 n 个盒子中相矛盾。证毕。

习 题 一②

1. 设 k_0 是给定的正整数，$P(n)$ 是关于正整数 n 的一种性质或命题。如果

(i) 当 $n=k_0$ 时，$P(k_0)$ 成立；

(ii) 由 $P(n)$ 成立可推出 $P(n+1)$ 成立，

那么，$P(n)$ 对所有正整数 $n\geqslant k_0$ 成立。

2. 在上题的条件下，如果

(i) 当 $n=k_0$ 时 $P(k_0)$ 成立；

(ii) 设 $n>k_0$。由对所有的 $m(k_0\leqslant m<n)P(m)$ 成立可推出 $P(n)$ 成立，

那么，$P(n)$ 对所有正整数 $n\geqslant k_0$ 成立。

3. 设 T 是一个由整数组成的集合。若 T 中有正整数，则 T 中必有最小正整数。

4. 设 T 是一个由整数组成的集合，若 T 有下界，即存在整数 a 使对所有的 $t\in T$，有 $t\geqslant a$，那么，必有 $t_0\in T$，使对所有的

---

① 亦称盒子原理。

② 做本章的习题必须按照以下要求：只能用这道题之前讲过的内容和做过的题去做，而不许用这道题以后讲的内容。这是为了更好的理解理论体系的逻辑结构。

$t \in T$ 有 $t \geqslant t_0$。

5．设M是一个由整数组成的集合。若M有上界，即存在整数 a，使对所有的 $m \in M$ 有 $m \leqslant a$，那么，必有 $m_0 \in M$，使对所有的 $m \in M$ 有 $m \leqslant m_0$。

6．设 $a \geqslant 2$ 是给定的正整数。证明：对任一正整数 n 必有唯一的整数 $k \geqslant 0$，使 $a^k \leqslant n < a^{k+1}$。

§2 整　　除

定义1 设 $a, b \in \boldsymbol{Z}$，$a \neq 0$。如果存在 $q \in \boldsymbol{Z}$ 使得 $b = aq$，那么就说 b 可被 a 整除，记作 $a \mid b$，且称 b 是 a 的倍数，a 是 b 的约数（也可称为除数、因数）。b 不能被 a 整除就记作 $a \nmid b$。

由定义及乘法运算的性质，立即可推出整除关系有下面性质（注意：符号 $a \mid b$ 本身包含了条件 $a \neq 0$）。

定理1 (i) $a \mid b \Longleftrightarrow -a \mid b \Longleftrightarrow a \mid -b \Longleftrightarrow |a| \mid |b|$；

(ii) $a \mid b$ 且 $b \mid c \Longrightarrow a \mid c$；

(iii) $a \mid b$ 且 $a \mid c \Longleftrightarrow$ 对任意的 $x, y \in \boldsymbol{Z}$ 有 $a \mid bx + cy$；

(iv) 设 $m \neq 0$。那么，$a \mid b \Longleftrightarrow ma \mid mb$；

(v) $a \mid b$ 且 $b \mid a \Longrightarrow b = \pm a$；

(vi) 设 $b \neq 0$。那么，$a \mid b \Longrightarrow |a| \leqslant |b|$。

证 由 $b = aq \Longleftrightarrow b = (-a)(-q) \Longleftrightarrow -b = a(-q) \Longleftrightarrow |b| = |a||q|$ 就证明了(i)。因由 $b = aq_1$ 和 $c = bq_2$ 可推出 $c = a(q_1q_2)$，就证明了(ii)。由 $b = aq_1, c = aq_2$ 可推出 $bx + cy = a(q_1x + q_2y)$，这就证明了(iii)的必要性。取 $x = 1, y = 0$ 及 $x = 0, y = 1$ 就可推出(iii)的充分性。由乘法相消律知，当 $m \neq 0$ 时，$b = aq \Longleftrightarrow mb = (ma)q$，这就证明了(iv)。由 $b = aq_1$ 和 $a = bq_2$ 就推出 $a = a(q_1q_2)$，由此及 $a \neq 0$ 推出 $q_1q_2 = 1$。所以 $q_1 = \pm 1$。这就证明了(v)。由(i)知，从 $a \mid b$ 可推出 $|b| = |a||q|$。由 $b \neq 0$ 知 $|q| \geqslant 1$，这就证明了(vi)。

例1 证明：若 $3 \mid n$ 且 $7 \mid n$，则 $21 \mid n$。

由$3|n$知$n=3m$，所以$7|3m$。由此及$7|7m$得$7|(7m-2\cdot 3m)=m$。因而有$21|n$。

例2 设$a=2t-1$。若$a|2n$，则$a|n$。

由$a|2tn$及$2tn=an+n$得$a|(2tn-an)$，即$a|n$。

例3 设a,b是两个给定的非零整数，且有整数x,y，使得$ax+by=1$。证明：若$a|n$且$b|n$，则$ab|n$。

由$n=n(ax+by)=(na)x+(nb)y$，及$ab|na,ab|nb$即得所要结论。注意到$7\cdot 1+3\cdot(-2)=1$，由此也证明了例1。

例4 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$是整系数多项式。若$d|b-c$，则$d|f(b)-f(c)$。

我们有

$$f(b)-f(c)=a_n(b^n-c^n)+a_{n-1}(b^{n-1}-c^{n-1})+\cdots+a_1(b-c),$$

由此及$d|b^j-c^j$，就推出所要结论。

由定义知，一个整数$a\neq 0$，它的所有倍数是

$$qa,\quad q=0,\pm 1,\pm 2,\cdots,$$

这个集合是完全确定的。零是所有非零整数的倍数。但对于一个整数$b\neq 0$，关于它的约数一般就知道得不多了。显见，$\pm 1,\pm b$（当$b=\pm 1$时只有两个）一定是b的约数，它们称为是b的**显然约(因、除)数**；b的其它的约数（如果有的话）称为是b的**非显然约(因、除)数**，或**真约(因、除)数**。由定理1(vi)知，$b\neq 0$的约数个数只有有限个。例如，$b=12$时，它的全体约数是：

$$\pm 1,\pm 2,\pm 3,\pm 4,\pm 6,\pm 12,$$

其中非显然约数有8个。$b=7$时，它的全体约数是：

$$\pm 1,\quad \pm 7,$$

它没有非显然约数。下面关于约数的性质是有用的。

定理2 设整数$b\neq 0,d_1,d_2,\cdots,d_k$是它的全体约数。那么，$b/d_1,b/d_2,\cdots,b/d_k$也是它的全体约数。也就是说，当$d$遍历$b$

的全体约数时，b/d 也遍历 b 的全体约数。此外，若 $b>0$，则当 d 遍历 b 的全体正约数时，b/d 也遍历 b 的全体正约数。

证 当 $d_j|b$ 时，b/d_j 是整数，$b=d_j(b/d_j)$，所以 b/d_j 也是 b 的约数，且当 $d_i\neq d_j$ 时，$b/d_i\neq b/d_j$。这样，$b/d_1,\cdots,b/d_k$ 是 k 个两两不同的 b 的约数。由于 b 的约数的个数是一定的，这就证明了第一个结论。只要注意到 b 的正约数的个数也是一定的（由定理1(i)知，所有的约数中一半是正的、一半是负的），由同样的讨论就推出第二个结论。

例如，$b=12$时，我们有

$$d=\pm1,\pm2,\pm3,\pm4,\pm6,\pm12.$$

$$b/d=\pm12,\pm6,\pm4,\pm3,\pm2,\pm1.$$

上面已经看到，有的数（例如7）只有显然约数。这种数在整数中有特别重要的作用。为此引进

定义2 设整数 $p\neq0,\pm1$。如果它除了显然约数 $\pm1,\pm p$ 外没有其它的约数，那么，p 就称为是不可约数，也叫作素数。若 $a\neq0,\pm1$且 a 不是不可约数，则 a 称为合数。

当 $p\neq0,\pm1$时，由于 p 和 $-p$ 必同为不可约数或合数，所以，以后若没有特别说明，不可约数（素数）总是指正的。例如

$$2,3,5,7,11,13,17,19,23,29,31$$

都是不可约数。由定义立即推出（读者自己证明）：

定理3 (i) $a>1$ 是合数的充要条件是 $a=de,1<d<a,1<e<a$；

(ii) 若 $d>1,q$ 是不可约数且 $d|q$，则 $d=q$。

定理4 若 a 是合数，则必有不可约数 $p|a$。

证 由定义知 a 必有除数 $d\geq2$。设集合 T 由 a 的所有除数 $d\geq2$组成。由最小自然数原理知集合 T 中必有最小的自然数，设为 p。p 一定是不可约数。若不然，$p\geq2$是合数，由定理3(i)知 p 必有除数 d'：$2\leq d'<p$。显然 d' 属于T，这和 p 的最小性矛盾。证毕。

一个整数的除数如果是不可约数（即素数），那么这个除数就称为不可约除(因)数或素除(因)数。

定理5 设整数 $a\geqslant2$。那么，a 一定可表为不可约数的乘积（包括 a 本身是不可约数），即

$$a=p_1p_2\cdots p_s, \qquad (1)$$

其中 $p_j(1\leqslant j\leqslant s)$是不可约数。

证 我们用第二种数学归纳法来证。当 $a=2$ 时，2是不可约数，所以结论成立。假设对某个 $n>2$，当$2\leqslant a<n$ 时，结论对所有这种 a 都成立。当 $a=n$ 时，若 n 是不可约数，则结论成立；若 n 是合数，则必有 $n=n_1n_2,2\leqslant n_1,n_2<n$。由假设知 n_1,n_2 都可表为不可约数的乘积：

$$n_1=p_{11}\cdots p_{1s}, \quad n_2=p_{21}\cdots p_{2r}.$$

这样，就把 a 表为不可约数的乘积：

$$a=n=n_1n_2=p_{11}\cdots p_{1s}p_{21}\cdots p_{2r}.$$

因此，由第二种数学归纳法知，定理对所有的 $a\geqslant2$都成立。

例如，1260的不相同的不可约除数有2，3，5，7，共四个。

$$1260=2\cdot2\cdot3\cdot3\cdot5\cdot7=2^2\cdot3^2\cdot5\cdot7,$$

所以，1260共有6个不可约除数（包括相同的）。从定理5容易推出(证明留给读者)：

推论6 设整数 $a\geqslant2$。

(i) 若 a 是合数，则必有不可约数 $p|a,p\leqslant a^{1/2}$；

(ii) 若 a 有表示式(1)，则必有不可约数 $p|a,p\leqslant a^{1/s}$。

例如，当 $a=1260$时，$s=6$。它的不可约除数 2 就满足

$$2<(1260)^{1/6}\approx3.28\cdots.$$

推论6给出了一个寻找不可约数的有效算法。例如，为了求出不超过100（或任给的正整数N）的所有不可约数，只要把1，及不超过100(或N）的所有正合数都删去。由推论6知，不超过100(或N)的正合数 a 必有一个不可约除数 $p\leqslant a^{1/2}\leqslant100^{1/2}=10$（或 $N^{1/2}$），因而，只要先求出不超过 10（或 $N^{1/2}$)的全部不可

约数2,3,5,7（或 $p_1,p_2,\cdots,p_s$），然后，依次把不超过100（或N）的正整数中的除了2,3,5,7（或 $p_1,\cdots,p_s$）以外的 2 的倍数、3 的倍数、5 的倍数、7 的倍数（或 p_1 的倍数，…，p_s 的倍数）全部删去，就删去了不超过 100（或N）的全部正合数，剩下的正好就是不超过100（或N）的全部不可约数。具体做法见下表，取$N=100$

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~								

由上表可以看出，没有删去的数是

2,3,5,7,11,13,17,19,23,29,31,37,41,43,

47,53,59,61,67,71,73,79,83,89,97,

共有25个，它们就是不超过100的全部不可约数。从这不超过100的25个素数出发，重复上面的做法，就可找出不超过$100^2=10000$的全部素数。这种寻找不可约数的方法，通常叫做Eratoschenes筛法。

数学中的一个著名的定理是：

定理7 不可约数有无穷多个。

证 用反证法。假设只有有限个不可约数（注意：已约定不可约数一定是正的），它们是 $q_1,\cdots,q_k$。考虑 $a=q_1q_2\cdots q_k+1$。显见，$a>2$。由定理 4 知必有不可约数 $p|a$。由假设知 p 必等于某个 q_j，因而 $p=q_j$一定整除 $a-q_1q_2\cdots q_k=1$，但不可约数 $q_j\geqslant2$，

这是不可能的，矛盾。因此，假设是错误的，即不可约数必有无穷多个。证毕。

设 $q_1=2, q_2=3, q_3=5, q_4, q_5, \cdots$ 是全体不可约数按大小顺序排成的序列，以及

$$Q_k = q_1 q_2 \cdots q_k + 1.$$

由直接计算得（q_j 已在上面求出）：

$$Q_1=3, Q_2=7, Q_3=31, Q_4=211, Q_5=2311,$$
$$Q_6=59\cdot 509, Q_7=19\cdot 97\cdot 277, Q_8=347\cdot 27953,$$
$$Q_9=317\cdot 703763, Q_{10}=331\cdot 571\cdot 34231,$$

这里前五个是不可约数，后五个是合数，但 Q_k 都有一个比 q_k 更大的不可约除数。至今还不知道是否有无穷多个 k 使 Q_k 是不可约数，也不知道是否有无穷多个 k 使 Q_k 是合数。

在初等数论书中，大多用“素数”这一术语而不用“不可约数”。虽然，从给出的定义 2 看，用“不可约数”这一名词更为贴切，但为了符合习惯，**下面我们将总用“素数”这一术语，且假定它是正的**。关于这两个名词的意义的讨论可参看附录二。

研究素数的性质是数论的核心问题之一，至今对这一问题还了解不多，我们将在第八章对素数的个数作初步的讨论。关于合数与素数的关系，一个立刻会想到的问题是：定理 5 中的表示式(I)在不计 $p_j(1\leqslant j\leqslant s)$ 次序的意义下是否是唯一的。回答是肯定的，这就是著名的算术基本定理（见 §6定理2）。证明这一定理的途径有两条：一是直接利用自然数的性质证明算术基本定理，并在此基础上建立关于整数的整除理论；另一是先建立包括最大公约数、最小公倍数等内容的关于整数的整除性质，然后推出算术基本定理。这两种途径都是很重要的，将在下面分别讨论。我们将先讨论第二种途径，因为这将使我们更清楚地认识与掌握初等数论中的基本概念和方法。

作为本节的结束，我们从定理 7 的证明来得到关于不超过 x 的素数个数——记作 $\pi(x)$——的一个很弱的下界估计，及第n个

素数p_n的大小的一个很弱的上界估计。

定理8 设全体素数按大小顺序排成的序列是：

$$p_1=2,\ p_2=3,\ p_3, p_4,\cdots. \tag{2}$$

我们有

$$p_n\leqslant 2^{2^{n-1}},\qquad n=1,2,\cdots, \tag{3}$$

及

$$\pi(x)>\log_2\log_2 x,\quad x\geqslant 2, \tag{4}$$

这里 $\log_2 y$表以 2 为底的对数。

证 由定理 7 的证明知

$$p_n\leqslant p_1p_2\cdots p_{n-1}+1,\quad n>1. \tag{5}$$

我们用归纳法来证(3)。当$n=1$时，式(3)显然成立。假设式(3)对$n\leqslant k(\geqslant 1)$成立，当$n=k+1$时，由式(5)及归纳假设得

$$p_{k+1}\leqslant 2^{2^0}\cdot 2^{2^1}\cdots 2^{2^{k-1}}+1=2^{2^k-1}+1<2^{2^k}.$$

即式(3)对$n=k+1$也成立。这就证明式(3)对任意的$n\geqslant 1$都成立。

下面来证式(4)。对 $x\geqslant 2$，必有唯一的正整数n，使得 $2^{2^{n-1}}\leqslant x<2^{2^n}$，因而有

$$\pi(x)\geqslant\pi(2^{2^{n-1}})\geqslant n,$$

最后一步用到了式(3).由此及 $x<2^{2^n}$就推出式(4)。

习 题 二

1.(i) 若 $a|b$ 且 $c|d$，则 $ac|bd$；

(ii) 若 $a|b_1,\cdots,a|b_k$，则对任意整数 $x_1,\cdots,x_k$有

$$a|b_1x_1+\cdots+b_kx_k.$$

2．若 $x^2+ax+b=0$ 有整数根 $x_0\neq 0$，则 $x_0|b$。一般地，若 $x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$ 有整数根 $x_0\neq 0$，则$x_0|a_0$。

3．判断以下方程有无整数根，若有整数根则求出所有这种根：

(i) $x^2+x+1=0$; (ii) $x^2-5x-4=0$;

(iii) $x^4+6x^3-3x^2+7x-6=0$; (iv) $x^3-x^2-4x+4=0$.

4. 有一种盒子能装3斤糖，另一种能装6斤糖。假定每个盒子必须装满，试问：能用这两种盒子来装完100斤糖吗？

5. 若$5|n$且$17|n$，则$85|n$。

6. 若$2|n$，$5|n$及$7|n$，则$70|n$。

7. 设$n\neq 1$。证明：$(n-1)^2|n^k-1$的充要条件是$(n-1)|k$。

8. 求以下各数的全部素除数、正除数、以及把它们表为素数的乘积：1234，2345，34560，111111。

9. 证明：(i) 设$n\geqslant 1$。2^n+1是素数的必要条件是$n=2^k$。

(ii) 2^n-1是素数的必要条件是n为素数。举出几个这两种形式的素数。

10. 证明：对任给的正整数K，必有K个连续正整数都是合数。

11. 证明：奇数一定能表为两平方数之差。

12. 设奇数$n>1$。证明：n是素数的充要条件是n不能表为三个或三个以上的相邻正整数之和。

13. 设p是正整数n的最小素因数。证明：若$p>n^{1/3}$，则n/p是素数。

14. 设$p_1\leqslant p_2\leqslant p_3$是素数，$n$是正整数。若$p_1p_2p_3|n$，则$p_1\leqslant n^{1/3}$，$p_2\leqslant(n/2)^{1/2}$。

15. 利用Eratoschenes筛法求出300以内的全部素数。

16. 利用第14题，提出一种类似于Eratoschenes筛法的方法，来求出所有不超过100且至多是两个素数乘积的正整数。

17. 设$n\geqslant 0$，$F_n=2^{2^n}+1$。再设$m\neq n$。证明：若$d>1$，且$d|F_n$，则$d\nmid F_m$。由此推出素数有无穷多个。

18. 设F_n同上题，证明：$F_{n+1}=F_n\cdots F_0+2$。

19. 设$A_1=2$，$A_{n+1}=A_n^2-A_n+1(n\geqslant 1)$。再设$n\neq m$。证明：若$d|A_n$，$d>1$，则$d\nmid A_m$。由此推出素数有无穷多个。

20. 设 A_n 同上题. 证明: $A_{n+1} = A_n \cdots A_1 + 1$.

21. 设$n \geqslant 3$. 证明: $n! - 1$ 的素因数$>n$. 由此推出素数有无穷多个. 并求最小的 n 使 $n! - 1$ 不是素数.

22. 设整系数多项式 $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $a_n \neq 0$. 证明: 必有无穷多个整数值x, 使得 $P(x)$是合数.

23. 证明: $n^2 + n + 41$ 当$n = 0, 1, 2, \cdots, 39$ 时都是素数.

24. 设 $k \geqslant 3$. 求出所有这样的正整数集合$\{a_1, \cdots, a_k\}$, 使得

(i) $a_1, \cdots, a_k$是两两不同的正整数,

(ii) 从中任意取出三个数, 它们的和可被这三个数中的任一个整除.

25. 设 $q \neq 0$, ± 1. 若对任意的 a, b, 由 $q|ab$ 可推出 $q|a$ 或 $q|b$至少有一个成立, 则q一定是不可约数.

26. 设a, b, n满足 $a|bn$, $ax + by = 1$, x, y是两个整数. 证明: $a|n$.

27. 设$m > 1$, $m|(m-1)! + 1$. 证明m是素数.

28. 假若素数只有有限个$p_1, \cdots, p_s$. 证明: 对任意正整数N必有

$$\sum_{n=1}^{N} \frac{1}{n} < \left(1 - \frac{1}{p_1}\right)^{-1} \cdots \left(1 - \frac{1}{p_s}\right)^{-1}.$$

由此推出素数有无穷多个.

29. 设整数$N \geqslant 2$. 证明:

(i) $\sum\limits_{p \leqslant N} \frac{1}{p-1} > \ln\ln(N+1)$, 这里求和号表示对所有不超过$N$的素数 p 求和;

(ii) $\sum\limits_{p \leqslant N} \frac{1}{p} > \ln\ln(N+1) - 1$.

30. 证明: (i) 任一正整数 a 一定可表为 $a = k^2 l$, 其中 k 是正整数, $l = 1$或是不同的素数的乘积.

(ii) 设整数 $N \geqslant 2$，则有 $N \leqslant \sqrt{N} \cdot 2^{\pi(N)}$.

(iii) $\pi(N) \geqslant (\log_2 N)/2$.

(iv) 第 n 个素数 $p_n \leqslant 2^{2^n}$.

§3 带余数除法

初等数论的证明中最重要、最基本、最直接的工具就是下面的带余数除法，也称为除法算法：

定理1 设a,b是两个给定的整数，$a \neq 0$。那么，一定存在唯一的一对整数 q与r，满足

$$b = qa + r, \quad 0 \leqslant r < |a|。\tag{1}$$

此外，$a|b$的充要条件是$r = 0$。

证 唯一性 若还有整数 q' 与r' 满足

$$b = q'a + r', \quad 0 \leqslant r' < |a|,\tag{2}$$

不妨设 $r' \geqslant r$。由式(1)和(2)得：$0 \leqslant r' - r < |a|$，及

$$r' - r = (q - q')a。$$

若 $r' - r > 0$，则由上式及 §2定理1(vi)推出$|a| \leqslant r' - r$.这和$r' - r < |a|$矛盾。所以，必有 $r' = r$，进而得$q' = q$。

存在性 当$a|b$时，可取 $q = b/a$，$r = 0$。当$a \nmid b$ 时，考虑集合

$$T = \{b - ka,\ k = 0, \pm 1, \pm 2, \cdots\}。$$

容易看出，集合T中必有正整数（例如，取 $k = -2|b|a$），所以由最小自然数原理知，T中必有一个最小正整数，设为

$$t_0 = b - k_0 a > 0。$$

我们来证明必有 $t_0 < |a|$。因$a \nmid b$所以 $t_0 \neq |a|$。若$t_0 > |a|$,则$t_1 = t_0 - |a| > 0$，显见，$t_1 \in T$，$t_1 < t_0$。这和t_0的最小性矛盾。取$q = k_0$，$r = t_0$就满足要求。

最后，显见当$b = qa + r$时，$a|b$的充要条件是$a|r$。当满足$0 \leqslant r < |a|$时，由 §2定理1(vi)就推出 $a|r$ 的充要条件是 $r = 0$。这就

证明了定理的最后一部分。证毕。

在具体应用带余数除法时，常取以下更灵活的形式：

定理2 设a,b是两个给定的整数，$a\neq0$，再设d是一给定的整数。那么，一定存在唯一的一对整数q_1与r_1，满足

$$b=q_1a+r_1,\qquad d\leqslant r_1<|a|+d. \tag{3}$$

此外，$a|b$的充要条件是$a|r_1$。

只要对a和$b-d$用定理1就可推出定理2，详细论证留给读者。特别有用的是取$d=-|a|/2$，当$2|a$；$d=-(|a|-1)/2$，当$2\nmid a$。这时式(3)变为

$$b=q_1a+r_1,$$

其中

$$\begin{cases}-|a|/2\leqslant r_1<|a|/2, & \text{当}2|a,\\ -(|a|-1)/2\leqslant r_1<(|a|+1)/2, & \text{当}2\nmid a.\end{cases}$$

合起来可写为

$$b=q_1a+r_1,\qquad -|a|/2\leqslant r_1<|a|/2. \tag{3$'$}$$

适当选取d（如何选？）也可使式（3）变为以下两种形式：

$$b=q_1a+r_1,\qquad -|a|/2<r_1\leqslant|a|/2\text{①}. \tag{3$''$}$$

$$b=q_1a+r_1,\qquad 1\leqslant r_1\leqslant|a|. \tag{3$'''$}$$

通常把式（1）中的r称为b被a除后的最小非负余数，式(3′)和(3″)中的r_1都称为绝对最小余数，式(3‴)中的r_1称为最小正余数，而式(3)中的r_1统称为余数。

推论3 设$a>0$，任一整数被a除后所得的最小非负余数是且仅是$0,1,\cdots,a-1$这a个数中的一个。

这是定理1的直接推论。它是常用的整数分类及进位制表示法的基础。

例1 设$a\geqslant2$是给定的正整数，$j=0,1,\cdots,a-1$。对给定的j，被a除后余数等于j的全体整数是

---

① 当a为奇数时式（3′）和（3″）是一样的。

$$ka+j,\quad k=0,\pm1,\pm2,\cdots。$$

这些整数组成的集合记为$S_{a,j}$。当$0\leqslant j\neq j'\leqslant a-1$时集合$S_{a,j}$和$S_{a,j'}$不相交，以及并集

$$S_{a,0}\cup S_{a,1}\cup\cdots\cup S_{a,a-1}=\boldsymbol{Z},$$

即全体整数按被a除后所得的最小非负余数来分类，分成了两两不相交的a个类。例如：$a=2$时，全体整数分为两类：

$$S_{2,0}=\{2k:\ k\in\boldsymbol{Z}\},\qquad S_{2,1}=\{2k+1:\ k\in\boldsymbol{Z}\};$$

$a=3$时全体整数分为三类：

$$S_{3,0}=\{3k:\ k\in\boldsymbol{Z}\},\qquad S_{3,1}=\{3k+1:k\in\boldsymbol{Z}\},$$
$$S_{3,2}=\{3k+2:k\in\boldsymbol{Z}\};$$

$a=6$时全体整数分为六类：

$$S_{6,0}=\{6k:k\in\boldsymbol{Z}\},\quad S_{6,1}=\{6k+1:k\in\boldsymbol{Z}\},S_{6,2}=\{6k+2:k\in\boldsymbol{Z}\},$$
$$S_{6,3}=\{6k+3:k\in\boldsymbol{Z}\},S_{6,4}=\{6k+4:k\in\boldsymbol{Z}\},S_{6,5}=\{6k+5:k\in\boldsymbol{Z}\}。$$

例 2 (i) $S_{2,0}\cap S_{3,0}=S_{6,0}$； (ii) $S_{2,1}\cap S_{3,1}=S_{6,1}$；
(iii) $S_{2,0}\cap S_{3,1}=S_{6,4}$。

先来证(i)。即要证$a=2k$且$a=3h$的充要条件是$a=6d$。充分性显然。由$2k=3h$知$h=2(k-h)$，所以$a=6(k-h)$。这就证明了必要性。

(ii) 就是要证：$a=2k+1$且$a=3h+1$的充要条件是$a=6d+1$，即$a-1=2k$且$a-1=3h$的充要条件是$a-1=6d$。而这正是(i)所证明的。

(iii) 就是要证：$a=2k$且$a=3h+1$的充要条件是$a=6d+4$。充分性显然。由$2k=3h+1$知$h=2(k-h)-1$，所以$a=6(k-h)-2=6(k-h-1)+4$，这就证明了必要性。请读者解释这些等式的含意。

例 3 $S_{2,1}=S_{6,1}\cup S_{6,3}\cup S_{6,5}$。

证 $n\in S_{2,1}$即$n=2k+1$，$k\in\boldsymbol{Z}$。而由例1知：必有$k=3h$，

$3h+1$或$3h+2$，$h\in\mathbf{Z}$，因而必有$n=6h+1$，$6h+3$或$6h+5$。反过来显然成立。请读者解释等式的含意。

例 4 设$a\geqslant2$是给定的正整数。那么，任一正整数n必可唯一表为

$$n=r_ka^k+r_{k-1}a^{k-1}+\cdots+r_1a+r_0,\qquad(4)$$

其中整数$k\geqslant0$，$0\leqslant r_j\leqslant a-1(0\leqslant j\leqslant k)$，$r_k\neq0$。这就是正整数的$a$进位表示。

证 对正整数n必有唯一的$k\geqslant0$，使$a^k\leqslant n<a^{k+1}$(为什么)。由带余数除法知，必有唯一的q_0，r_0满足

$$n=q_0a+r_0,\quad 0\leqslant r_0<a.$$

若$k=0$，则必有$q_0=0$，$1\leqslant r_0<a$，所以结论成立。设结论对$k=m\geqslant0$成立。那么，当$k=m+1$时，上式中的q_0必满足

$$a^m\leqslant q_0<a^{m+1}.$$

由假设知

$$q_0=s_ma^m+\cdots+s_0,$$

其中$0\leqslant s_j\leqslant a-1(0\leqslant j\leqslant m-1)$，$1\leqslant s_m\leqslant a-1$。因而有

$$n=s_ma^{m+1}+\cdots+s_0a+r_0,$$

即结论对$m+1$也成立。证毕。

例 5 设$a>2$是奇数。证明：

(i) 一定存在正整数$d\leqslant a-1$，使得$a\mid 2^d-1$。

(ii) 设d_0是满足(i)的最小正整数d。那么，$a\mid 2^h-1(h\in\mathbf{N})$的充要条件是$d_0\mid h$。

证 先证(i)。考虑以下a个数：

$$2^0,2^1,2^2,\cdots,2^{a-1}.$$

由§2例2知，$a\nmid 2^j(0\leqslant j<a)$。由此及定理1可得：对每个$j$，$0\leqslant j<a$，

$$2^j=q_ja+r_j,\quad 0<r_j<a.$$

所以a个余数$r_0,r_1,\cdots,r_{a-1}$仅可能取$a-1$个值。因此其中必有两个相等，设为r_i,r_k，不妨设$0\leqslant i<k<a$。因而有

$$a(q_k-q_i)=2^k-2^i=2^i(2^{k-i}-1).$$

利用§2的例2，由此推出 $a|2^{k-i}-1$。取 $d=k-i\leqslant a-1$ 就满足要求。

下面来证(ii)。充分性是显然的，只要证必要性。同样由定理1得

$$h=qd_0+r,\quad 0\leqslant r<d_0.$$

因而有

$$2^h-1=2^{qd_0+r}-2^r+2^r-1=2^r(2^{qd_0}-1)+(2^r-1).$$

由上式、$a|2^h-1$ 及 $a|2^{qd_0}-1$，就推出 $a|2^r-1$。由此及 d_0 的最小性就推出 $r=0$，即 $d_0|h$。

在例5中取 $a=11$，我们有

$2=0\cdot11+2$，$2^2=0\cdot11+4$，$2^3=0\cdot11+8$，$2^4=1\cdot11+5$，

$2^5=2\cdot11+10$，$2^6=5\cdot11+9$，$2^7=11\cdot11+7$，$2^8=23\cdot11+3$，

$2^9=46\cdot11+6$，$2^{10}=93\cdot11+1$。

因此，使 $11|2^d-1$ 的最小正整数 $d=10$，所有能使 $11|2^d-1$ 的正整数 $d=10\cdot k$，$k=1,2,\cdots$。由以上计算也可以看出，2^d 被11除后可能取到的最小非负余数是：1,2,3,4,5,6,7,8,9,10。

在例5中取 $a=15$，则有

$2=0\cdot15+2$，$2^2=0\cdot15+4$，$2^3=0\cdot15+8$，$2^4=1\cdot15+1$。

因此，使 $15|2^d-1$ 的最小正整数 $d=4$，所有能使 $15|2^d-1$ 的 $d=4\cdot k, k=1,2,3,\cdots$。由以上计算知，$2^d$ 被15除后可能取到的最小非负余数是：1,2,4,8。

推论3是对全体整数被一个固定的正整数 a 除后所得的最小非负余数的情况来说的。在例5中已经看到，特殊的整数或特殊的整数列被一个固定的正整数 a 除后所得的最小非负余数会有更特殊的性质，这一点在初等数论的论证中有重要作用。例如：

(i) 两个 $4k+3$ 形式的数（即被4除余3的数）的乘积一定是 $4k+1$ 形式的数（即被4除余1的数）；

(ii) x^2 被4除后所得的非负最小余数只可能是0，1；

(iii) x^2被8除后所得的非负最小余数只可能是0,4（当x为偶数），及1(当x为奇数)；

(iv) x^2被3除后所得的非负最小余数是0,1；

(v) x^3被9除后所得的非负最小余数是0,1,8。

请读者自己验证这些结论。这样，对任意的整数x,y，从(ii)可推出：$x^2+y^2\neq 4k+3$；从(iii)推出：$x^2+y^2\neq 8k+3$，$8k+6$，$8k+7$；从(v)推出：$x^3+y^3\neq 9k+3$，$9k+4$，$9k+5$，$9k+6$（请读者自己验证）。

以上证明的结论和所举例子都是对非负最小余数来说的。对绝对最小余数，以及一般指定的余数$d\leqslant r_1<|a|+d$（d为指定的整数），都可作同样的讨论。在应用中灵活地运用这一点是很重要的。

习 题 三

1. 证明§3定理2。设§3定理2中的$a>0$，那么，整数被a除后所得的余数r_1是且仅是$d,d+1,\cdots,d+a-1$这a个数中的一个。

2. 设$a>0$。证明：相邻的a个整数中有且仅有一个被a整除。

3. 分别写出被$-7,9,12$除后的所有最小非负余数、最小正余数和绝对最小余数。

4. (i) 若$2|ab$，则$2|a$，$2|b$至少有一个成立。

(ii) 若$7|ab$，则$7|a$，$7|b$至少有一个成立。

(iii) 若$14|ab$，试问$14|a$或$14|b$必有一个成立吗？

5. 设$a\neq 0,b_j=q_ja+s_j(1\leqslant j\leqslant n)$。证明：$b_1,\cdots,b_n$以任意方式作加、减、乘法运算后被$a$除后所得的最小非负余数等于$s_1,\cdots,s_n$以同样的方式作加、减、乘法运算后被$a$除后所得的最小非负余数。

6. 上题中的“最小非负余数”改为“绝对最小余数”、“最小正余数”、或§3定理2中的一般余数后，结论仍成立。

7. 证明：对任意整数 n 有

(i) $6|n(n+1)(n+2)$； (ii) $8|n(n+1)(n+2)(n+3)$；

(iii) $24|n(n+1)(n+2)(n+3)$；

(iv) 若$2\nmid n$，则$8|n^2-1$及$24|n(n^2-1)$；

(v) 若$2\nmid n$，$3\nmid n$，则$24|n^2+23$；(vi) $6|n^3-n$；

(vii) $30|n^5-n$；(viii) $42|n^7-n$；

(ix) 证明对任意整数n，$\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n$是整数。

8. 分别求出n^2, n^3, n^4, n^5被3,4,8,10除后，可能取到的最小非负余数、最小正余数及绝对最小余数。

9. 证明：(i) 对任意的整数x, y，必有$8\nmid x^2-y^2-2$；

(ii) 若$2\nmid xy$，则$x^2+y^2\neq n^2$；

(iii) 若$3\nmid xy$，则$x^2+y^2\neq n^2$；

(iv) 若$a^2+b^2=c^2$，则$6|ab$。

10. 设$a\geqslant 2$。对任一整数j，记$S_{a,j}=\{n=ka+j, k\in \boldsymbol{Z}\}$。证明：

(i) $S_{a,j_1}=S_{a,j_2}$的充要条件是$a|j_1-j_2$；

(ii) 当$a\nmid j_1-j_2$时，集合S_{a,j_1}和S_{a,j_2}不相交。

解释本题的含意。

11. 在上题的符号下，求j分别满足(i) $S_{3,0}\cap S_{5,0}=S_{15,j}$；

(ii) $S_{3,1}\cap S_{5,1}=S_{15,j}$；(iii) $S_{3,-1}\cap S_{5,-2}=S_{15,j}$。

12. 在第10题的符号下，求s及$j_1,\cdots,j_s$使得

$$S_{3,1}=S_{21,j_1}\cup\cdots\cup S_{21,j_s}.$$

一般地，设$a|b$，j为给定整数，求s及$j_1,\cdots,j_s$使得

$$S_{a,j}=S_{b,j_1}\cup\cdots\cup S_{b,j_s}.$$

解释本题的含意。

13. 证明：(i) $3k+1$形式的奇数一定是$6h+1$形式；

(ii) $3k-1$形式的奇数必是$6h-1$形式。

14. 证明：任一形如$3k-1$，$4k-1$，$6k-1$形式的正整数必

有同样形式的素因数。

15. 证明：(i) 形如$4k-1$的素数有无穷多个；

(ii) 形如$6k-1$的素数有无穷多个。

16. (a) 设$n=c_k\cdot10^k+\cdots+c_1\cdot10+c_0$。证明：(i) $2|n\Longleftrightarrow 2|c_0$；(ii) $5|n\Longleftrightarrow5|c_0$；(iii) $3|n\Longleftrightarrow3|(c_k+\cdots+c_0)$；(iv)$9|n\Longleftrightarrow9|(c_k+\cdots+c_0)$；(v) $11|n\Longleftrightarrow11|(c_k-c_{k-1}+\cdots+(-1)^k\cdot c_0)$。

(b) 设$n=c_k\cdot(100)^k+\cdots+c_1\cdot(100)+c_0$。证明：

(i) $11|n\Longleftrightarrow11|(c_k+\cdots+c_0)$；

(ii) $101|n\Longleftrightarrow n|(c_k-c_{k-1}+\cdots+(-1)^kc_0)$。

(c) 设$n=c_k\cdot(1000)^k+\cdots+c_1\cdot(1000)+c_0$。证明：(i) $37|n\Longleftrightarrow37|(c_k+\cdots+c_0)$； (ii) $7|n\Longleftrightarrow7|(c_k-c_{k-1}+\cdots+(-1)^k\cdot c_0)$；(iii) $13|n\Longleftrightarrow13|(c_k-c_{k-1}+\cdots+(-1)^kc_0)$。

(d) 利用以上各个结果提出相应的整数被2,3,5,7,9,11,13,37,或101整除的判别法。利用这种检查因数的方法，把1535625，1158066，82798848，81057226635000表成素数的乘积。

17. 设$n=10l+c_0$，$m=l-2c_0$。证明：$7|n\Longleftrightarrow7|m$。利用此法判断41283及第16题中的各数能否被7整除。

18. 设$h\geqslant0$是给定的整数，$a\geqslant2$。证明：

(i) 任一整数n，$0\leqslant n<a^{h+1}$，必可唯一地表为$n=r_ha^h+\cdots+r_1a+r_0$，$0\leqslant r_j\leqslant a-1$，$0\leqslant j\leqslant h$，且每一个这样表出的$n$满足$0\leqslant n<a^{h+1}$；

(ii) 若$a=3$，则任一整数n，$-(3^{h+1}-1)/2\leqslant n\leqslant(3^{h+1}-1)/2$，必可唯一地表为$n=r_h\cdot3^h+\cdots+r_1\cdot3+r_0$，$-1\leqslant r_j\leqslant1$，$0\leqslant j\leqslant h$，且每一个这样表出的$n$必满足$-(3^{h+1}-1)/2\leqslant n\leqslant(3^{h+1}-1)/2$。此外，当$n>0$时，第一个不为零的$r_j=1$，当$n<0$时，第一个不为零的$r_j=-1$；

(iii) 试求出表达式$n=r_h\cdot a^h+\cdots+r_1\cdot a+r_0(-a/2<r_j\leqslant a/2$，$0\leqslant j\leqslant h)$表出的整数$n$的范围；

(iv) 试求出表达式 $n=r_h\cdot a^h+\cdots+r_1\cdot a+r_0(-a/2\leqslant r_j<a/2,\ 0\leqslant j\leqslant h)$ 表出的整数 n 的范围；

(v) 当 a 为偶数，特别是 $a=2$ 时，比较(iii),(iv)所表出的整数范围的差别。

19. 设 $n\neq 0$。证明 n 必可唯一地表为：(i) $n=2^k\cdot m, 2\nmid m$；(ii) $n=3^k\cdot m, 3\nmid m$。

20. 设 $k\geqslant 1$。证明：(i) 若 $2^k\leqslant n<2^{k+1}$，及 $1\leqslant a\leqslant n, a\neq 2^k$，则 $2^k\nmid a$；

(ii) 若 $3^k\leqslant 2n-1<3^{k+1}, 1\leqslant l\leqslant n, 2l-1\neq 3^k$，则 $3^k\nmid 2l-1$。

21. 证明：当 $n>1$ 时，$1+1/2+\cdots+1/n$ 不是整数。

22. 证明：当 $n>1$ 时，$1+1/3+1/5+\cdots+1/(2n-1)$ 不是整数。

23. 在任意给定的两个以上的相邻正整数中必有唯一的一个正整数 $a=2^r\cdot m, 2\nmid m$，使得 2^r 不能整除其它正整数。

24. 设 m,n 是正整数。证明：不管如何选取"+"、"−"号，$\pm 1/m\pm 1/(m+1)\pm\cdots\pm 1/(m+n)$ 一定不是整数。

25. 设 $n>1$。证明：n 可表为两个或两个以上的相邻正整数之和的充要条件是 $n\neq 2^k$。

26. 设 $m>n$ 是正整数。证明：$2^n-1\mid 2^m-1$ 的充要条件是 $n\mid m$。以任一正整数 $a>2$ 代替 2 结论仍然成立吗？

27. 设 a,b 是正整数，$b>2$。证明：$2^b-1\nmid 2^a+1$。

28. 设 $a\geqslant 2$，$m\geqslant 2$，满足 $ax+my=1$，其中 x,y 为某两个整数。证明：

(i) 一定存在正整数 $d\leqslant a-1$ 使得 $a\mid m^d-1$；

(ii) 设 d_0 是满足(i)的最小正整数 d。那么，$a\mid m^h-1(h\in\boldsymbol{N})$ 的充要条件是 $d_0\mid h$。

29. 求(i) $7\mid 2^d-1$ 的最小正整数 d；(ii) $11\mid 3^d-1$ 的最小正整数 d；(iii) 2^d 被7除后所可能取到的最小非负余数，绝对最小余数；(iv) 3^d 被11除后所可能取到的最小非负余数，绝对最小

余数。

30．证明：对任意正整数d，

(i) $13 \nmid 3^d, 3^d+1, 3^d \pm 2, 3^d+3, 3^d-4, 3^d \pm 5, 3^d \pm 6$；

(ii) $13 \nmid 4^d, 4^d \pm 2, 4^d \pm 5, 4^d \pm 6$。

31．证明：不存在整数k使得：(i) $x^2+2y^2=8k+5, 8k+7$；

(ii) $x^2-2y^2=8k+3, 8k+5$；(iii) $x^2+y^2+z^2=8k+7$；

(iv) $x^3+y^3+z^3=9k\pm 4$；(v) $x^3+2y^3+4z^3=9k^3$。

32．设奇数$a>2$，$a\mid 2^d-1$的最小正整数$d=d_0$。证明：2^d被a除后，所可能取到的不同的最小非负余数有d_0个。

§4 最大公约数与最小公倍数

定义1 设a_1, a_2是两个整数。如果$d\mid a_1$且$d\mid a_2$，那么，d就称为是a_1和a_2的**公约数**。一般地，设$a_1, a_2, \cdots, a_k$是k个整数。如果$d\mid a_1, \cdots, d\mid a_k$，那么，$d$就称为是$a_1, \cdots, a_k$的**公约数**。

例如：$a_1=12, a_2=18$。它们的公约数是$\pm 1, \pm 2, \pm 3, \pm 6$。$a_1=6, a_2=10, a_3=-15$。它们的公约数是$\pm 1$。$n$和$n+1$的公约数是$\pm 1$。当$a_1, \cdots, a_k$中有一个不为零时，它们的公约数的个数有限。因此，可引进：

定义2 设a_1, a_2是两个不全为零的整数。我们把a_1和a_2的公约数中的最大的称为a_1和a_2的**最大公约数**，记作(a_1, a_2)。一般地，设$a_1, \cdots, a_k$是k个不全为零的整数。我们把$a_1, \cdots, a_k$的公约数中的最大的称为$a_1, \cdots, a_k$的最大公约数，记作$(a_1, \cdots, a_k)$。我们用$\mathscr{D}(a_1, \cdots, a_k)$表$a_1, \cdots, a_k$的所有公约数组成的集合。这样就有

$$(a_1, a_2)=\max(d:\ d\in\mathscr{D}(a_1, a_2)), \tag{1}$$

$$(a_1, \cdots, a_k)=\max(d:\ d\in\mathscr{D}(a_1, \cdots, a_k)). \tag{2}$$

前面所举的例子表明：$\mathscr{D}(12, 18)=\{\pm 1, \pm 2, \pm 3, \pm 6\}$，

$(12,18)=6$; $\mathscr{D}(6,10,-15)=\{\pm 1\}$, $(6,10,-15)=1$, $(n,n+1)=1$. 由定义立即推出以下性质：

定理1 (i) $(a_1,a_2)=(a_2,a_1)=(-a_1,a_2)$; 一般地,

$$(a_1,a_2,\cdots,a_i,\cdots,a_k)=(a_i,a_2,\cdots,a_1,\cdots,a_k)$$
$$=(-a_1,a_2,\cdots,a_k);$$

(ii) 若 $a_1|a_j$, $j=2,\cdots,k$, 则

$$(a_1,a_2)=(a_1,a_2,\cdots,a_k)=|a_1|;$$

(iii) 对任意的整数 x, $(a_1,a_2)=(a_1,a_2,a_1x)$;

$$(a_1,\cdots,a_k)=(a_1,\cdots,a_k,a_1x);$$

(iv) 对任意整数 x, $(a_1,a_2)=(a_1,a_2+a_1x)$,

$$(a_1,a_2,a_3,\cdots,a_k)=(a_1,a_2+a_1x,a_3,\cdots,a_k);$$

(v) 若 p 是素数，则

$$(p,a_1)=\begin{cases} p, & p|a_1, \\ 1, & p\nmid a_1; \end{cases}$$

一般地

$$(p,a_1,\cdots,a_k)=\begin{cases} p, & p|a_j, \quad j=1,2,\cdots,k, \\ 1, & \text{其它}. \end{cases}$$

证 根据公约数的定义及整除性质推出：

$$\mathscr{D}(a_1,a_2)=\mathscr{D}(a_2,a_1)=\mathscr{D}(-a_1,a_2),$$
$$\mathscr{D}(a_1,a_2)=\mathscr{D}(a_1,a_2,a_1x), \quad x\in\boldsymbol{Z},$$
$$\mathscr{D}(a_1,a_2)=\mathscr{D}(a_1,a_2+a_1x), \quad x\in\boldsymbol{Z},$$

由此及最大公约数的定义就分别证明了(i),(iii), (iv)当 $k=2$ 时成立，$k>2$ 的情形同样证明。(ii)由 §1 定理 1 的(vi)推出。(v)由素数的定义及(ii)推出。

下面举例说明，如何用定理 1 来求最大公约数。

例1 (i) 对任意的整数 n 有

$(21n+4,\ 14n+3)=(7n+1,14n+3)=(7n+1,1)=1$.

(ii) 对任意整数 n 有

$$(n-1,n+1)=(n-1,2)=\begin{cases}1, & 2\mid n,\\ 2, & 2\nmid n.\end{cases}$$

(iii) $(30,45,84)=(30,15,84)=(0,15,84)$

$$=(15,84)=(15,-6)=(3,-6)=3.$$

(iv) 对任意整数 n 有，

$$(2n-1,n-2)=(2n-1-2(n-2),n-2)=(3,n-2)$$

$$=(3,n-2-3(n-1))=(3,2n-1)$$

$$=\begin{cases}3, & n=3k+2,\\ 1, & n=3k\text{或}3k+1.\end{cases}$$

(v) 设 a,m,n 是正整数，$m>n$。由 $a^{2^n}+1\mid a^{2^m}-1$知，

$$(a^{2^m}+1,\ a^{2^n}+1)=(a^{2^m}-1+2,a^{2^n}+1)$$

$$=(2,a^{2^n}+1)$$

$$=\begin{cases}1, & 2\mid a,\\ 2, & 2\nmid a.\end{cases}$$

例 2 设 a 是奇数。证明：必有正整数 d 使 $(2^d-3,a)=1$。

证 由 § 3例 5(i)知，必有 d 使 $a\mid 2^d-1$。因而有

$$(2^d-3,a)=(2^d-1-2,a)=(-2,a)=1.$$

一组数的最大公约数等于 1 是刻画这组数之间关系的一个重要性质。为此引进

定义3 若$(a_1,a_2)=1$，则称 a_1 和 a_2 是既约的，也称 a_1和 a_2 是互素的。一般地，若$(a_1,\cdots,a_k)=1$，则称 $a_1,\cdots,a_k$ 是既约的，也称 $a_1,\cdots,a_k$ 是互素的。

例如：2 和 $2n+1$ 既约；对任意的 n, $21n+4$ 和$14n+3$既约；$6,10,-15$是既约的，但它们中任意两个数不既约，因为$(6,10)=2,(10,-15)=5,(-15,6)=3$。下面的定理对判断一组数是否既约是有用的。

定理2 如果存在整数 $x_1,\cdots,x_k$，使得

$$a_1x_1+\cdots+a_kx_k=1, \tag{3}$$

则 $a_1,\cdots,a_k$ 是既约的。

证 因为 $a_1,\cdots,a_k$ 的任一公约数 d 一定要整除 1，所以，必有 $d=\pm1$。这就证明了所要的结论。

以后将证明条件(3)也是 $a_1,\cdots,a_k$ 既约的必要条件。利用定理 2 也可证例 1(i)的结论，因为

$$3\cdot(14n+3)+(-2)(21n+4)=1.$$

由定义还可推出最大公约数以下的性质。

定理3 设正整数 $m\mid(a_1,\cdots,a_k)$。我们有

$$m(a_1/m,\cdots,a_k/m)=(a_1,\cdots,a_k). \tag{4}$$

特别地有

$$\left(\frac{a_1}{(a_1,\cdots,a_k)},\cdots,\frac{a_k}{(a_1,\cdots,a_k)}\right)=1. \tag{5}$$

证 记 $D=(a_1,\cdots,a_k)$。由 $m\mid D$，$D\mid a_j\ (1\leqslant j\leqslant k)$ 知 $m\mid a_j\ (1\leqslant j\leqslant k)$，因而有

$$(D/m)\mid(a_j/m),\quad j=1,\cdots,k,$$

即 D/m 是 $a_1/m,\cdots,a_k/m$ 的公约数，且是正的，所以由定义知

$$D/m\leqslant(a_1/m,\cdots,a_k/m). \tag{6}$$

另一方面，若 $d\mid(a_j/m),1\leqslant j\leqslant k$，则 $md\mid a_j,j=1,\cdots,k$，由定义知

$$md\leqslant D,\ \text{即}\ d\leqslant D/m.$$

取 $d=(a_1/m,\cdots,a_k/m)$，由此及式(6)即得式(4)。在式(4)中取 $m=(a_1,\cdots,a_k)$ 即得式(5)。

以后将证明：以条件 $m\mid a_j\ (1\leqslant j\leqslant k)$ 代替条件 $m\mid(a_1,\cdots,a_k)$ 时，式(4)仍然成立。

定义4 设 a_1,a_2 是两个均不等于零的整数。如果 $a_1\mid l$ 且 $a_2\mid l$，则称 l 是 a_1 和 a_2 的公倍数。一般地，设 $a_1,\cdots,a_k$ 是 k 个均不等于零的整数。如果 $a_1\mid l,\cdots,a_k\mid l$，则称 l 是 $a_1,\cdots,a_k$ 的公倍数。此外，以 $\mathscr{L}(a_1,\cdots,a_k)$ 记 $a_1,\cdots,a_k$ 的所有公倍数组成的集合。

例如：$a_1=2,a_2=3$。由§3例2(i)知，它们的公倍数集合

$$\mathscr{L}(2,3)=\{0,\pm 6,\pm 12,\cdots,\pm 6k,\cdots\}。$$

由最小自然数原理知，可引进以下的概念：

定义5 设整数 a_1,a_2 均不为零。我们把 a_1 和 a_2 的正的公倍数中的最小的称为 a_1 和 a_2 的**最小公倍数**，记作$[a_1,a_2]$，即

$$[a_1,a_2]=\min\{l:l\in\mathscr{L}(a_1,a_2),l>0\}。\tag{7}$$

一般地，设整数 $a_1,\cdots,a_k$ 均不等于零。我们把 $a_1,\cdots,a_k$ 的正的公倍数中的最小的称为 $a_1,\cdots,a_k$ 的**最小公倍数**，记作$[a_1,\cdots,a_k]$，即

$$[a_1,\cdots,a_k]=\min\{l:l\in\mathscr{L}(a_1,\cdots,a_k),l>0\}。\tag{8}$$

例如：$[2,3]=6$。由定义立即推得

定理4 (i) $[a_1,a_2]=[a_2,a_1]=[-a_1,a_2]$；一般地有

$$[a_1,a_2,\cdots,a_j,\cdots,a_k]=[a_j,a_2,\cdots,a_1,\cdots,a_k]$$
$$=[-a_1,a_2,\cdots,a_j,\cdots,a_k]；$$

(ii) 若 $a_2|a_1$ 则$[a_1,a_2]=|a_1|$；若 $a_j|a_1$ $(2\leqslant j\leqslant k)$，则

$$[a_1,\cdots,a_k]=|a_1|；$$

(iii) 对任意的 $d|a_1$，

$$[a_1,a_2]=[a_1,a_2,d]；\qquad [a_1,\cdots,a_k]=[a_1,\cdots,a_k,d]。$$

证明留给读者。

定理5 设 $m>0$。我们有

$$[ma_1,\cdots,ma_k]=m[a_1,\cdots,a_k]。\tag{9}$$

证 设 $L=[ma_1,\cdots,ma_k]$，$L'=[a_1,\cdots,a_k]$。由 $ma_j|L(1\leqslant j\leqslant k)$推出 $a_j|L/m(1\leqslant j\leqslant k)$，进而由最小公倍数定义知 $L'\leqslant L/m$。另一方面，由 $a_j|L'(1\leqslant j\leqslant k)$ 推出 $ma_j|mL'(1\leqslant j\leqslant k)$，进而由最小公倍数定义推出 $L\leqslant mL'$。这就证明了式(9)。

习 题 四 (Ⅰ)

1．求以下数组的全体公约数，并由此求出它们的最大公约数：

(i) $72,-60$；　(ii) $-120,28$；　(iii) $168,-180,495$。

2．给出四个整数，它们的最大公约数是1，但任何三个数都不既约。

3．证明：(i) $(a,b,c)\leqslant(a,b)$，$[a,b,c]\geqslant[a,b]$；

(ii) 若 $a|b$，则 $[a,c]\leqslant[b,c]$，$(a,c)\leqslant(b,c)$；

(iii) $(a,b)\leqslant(a+b,a-b)$；

(iv) $(a,b)\leqslant(ax+by,\ au+bv)$，$x,y,u,v$ 是任意整数。

4．若 $(a,b)=1,c|a+b$，则 $(c,a)=(c,b)=1$。

5．设 $n\geqslant1$。证明：$(n!+1,(n+1)!+1)=1$。

6．求最大公约数

(i) $(2t+1,2t-1)$；　(ii) $(2n,2(n+1))$；

(iii) $(kn,k(n+2))$；　(iv) $(n-1,n^2+n+1)$。

7．设 a,b 是正整数。证明：若 $[a,b]=(a,b)$，则 $a=b$。

8．证明：若 $(a,4)=(b,4)=2$，则 $(a+b,4)=4$。

9．设整数 a,b,c,d 满足 $ad-bc=\pm1$。证明：若 $u=am+bn$，$v=cm+dn$，则 $(m,n)=(u,v)$。

10．设 a,b 是正整数，且有整数 x,y 使得 $ax+by=1$。证明：

(i) $[a,b]=ab$；(ii) $(ac,b)=(c,b)$。

11．若 $2\nmid b$，则 $(2^ka,b)=(a,b)$。

12．设 g,l 是给定的正整数。证明：

(i) 存在整数 x,y 使得 $(x,y)=g$，$[x,y]=l$ 的充要条件是 $g|l$；

(ii) 存在正整数 x,y 使得 $(x,y)=g,xy=l$ 的充要条件是 $g^2|l$。

13．求满足 $(a,b)=10$，$[a,b]=100$ 的全部正整数组 a,b。

14．求满足 $[a,b,c]=10$ 的全部正整数组 a,b,c。

15．求满足 $(a,b,c)=10$，$[a,b,c]=100$ 的全部正整数组 a,b,c。

16．求以下数组的最小公倍数：(i) $198,252$；(ii) $482,1687$。

17．设 a,b 是正整数。那么，$a,2a,3a,\cdots$中第一个被 b 整除的数就是$[a,b]$。如何把这方法推广来求$[a_1,\cdots,a_k]$？

18．设 $n\geqslant1$．以 $\phi(n)$记正整数 $1,2,\cdots,n$中与 n 既约的数的个数。证明：

(i) $\phi(1)=\phi(2)=1$；

(ii) 当 $n\geqslant3$ 时，$2|\phi(n)$；

(iii) 当 $n=p$ 为素数时，$\phi(p)=p-1$。

以下要证明的关于最大公约数、最小公倍数的性质都要用到带余数除法（§3定理1）。

定理6 $a_j|c(1\leqslant j\leqslant k)$的充要条件是$[a_1,\cdots,a_k]|c$。

证 充分性是显然的。下证必要性。设 $L=[a_1,\cdots,a_k]$。由§3定理1知，有 q,r 使得

$$c=qL+r,\quad 0\leqslant r<L.$$

由此及 $a_j|c$ 推出 $a_j|r(1\leqslant j\leqslant k)$，所以 r 是公倍数。进而，由最小公倍数的定义及 $0\leqslant r<L$ 就推出 $r=0$，即 $L|C$，这就证明了必要性。结论表明：**公倍数一定是最小公倍数的倍数。**

定理7 设D是正整数。那么，$D=(a_1,\cdots,a_k)$的充要条件是：(i) $D|a_j(1\leqslant j\leqslant k)$，(ii) 若 $d|a_j(1\leqslant j\leqslant k)$，则$d|D$。

证 充分性 由(i)知D是$a_j(1\leqslant j\leqslant k)$的公约数，由(ii)、§2定理1(vi)、及 $D\geqslant1$ 知，$a_j(1\leqslant j\leqslant k)$的任一公约数 d 有$|d|\leqslant D$。因而由定义知D是 $a_1,\cdots,a_k$ 的最大公约数。

必要性 设 $d_1,\cdots,d_s$ 是 $a_1,\cdots,a_k$ 的全体公约数，$L=[d_1,\cdots,d_s]$。由定理6知 $L|a_j(1\leqslant j\leqslant k)$，因此，$L$满足条件(i)和(ii)(取 $D=L$)。因而，由上面证明的充分性知$L=(a_1,\cdots,a_k)=D$。这就证明了必要性。结论表明：**公约数一定是最大公约数的约数。**

定理8 设 $m>0$，我们有

$$m(b_1,\cdots,b_k)=(mb_1,\cdots,mb_k).\tag{10}$$

证 在定理3中取 $a_j=mb_j(1\leqslant j\leqslant k)$，由定理7就推出 $m\mid(a_1,\cdots,a_k)$。因此式(4)成立，即式(10)成立。证毕。

定理9 (i) $(a_1,a_2,a_3,\cdots,a_k)=((a_1,a_2),a_3,\cdots,a_k)$；

(ii) $(a_1,\cdots,a_{k+r})=((a_1,\cdots,a_k),(a_{k+1},\cdots,a_{k+r}))$①。

证 我们来证(i)。若 $d\mid a_j(1\leqslant j\leqslant k)$，则由定理7($k=2$)知，$d\mid(a_1,a_2),d\mid a_j(3\leqslant j\leqslant k)$；反过来，若 $d\mid(a_1,a_2),d\mid a_j(3\leqslant j\leqslant k)$，则由定义知，$d\mid a_j(1\leqslant j\leqslant k)$。这就是证明了

$$\mathscr{D}(a_1,a_2,a_3,\cdots,a_k)=\mathscr{D}((a_1,a_2),a_3,\cdots,a_k).$$

所以(i)成立。由(i)即推出(ii) 详细证明留给读者。

定理9表明：多个数的最大公约数，可以由求两个数的最大公约数来逐步求出。定理8表明：求一组数的最大公约数时可以通过提出这组数的公约数的方法来逐步求出。这正是我们所熟知的求最大公约数的方法，这里给出了严格的证明。例如：

$$(12,18)=2\cdot(6,9)=2\cdot3\cdot(2,3)=6\cdot(2,3-2)=6\cdot(2,1)=6.$$

这里还用到了定理1．再例如，

$$(6,10,-15)=((6,10),15),$$

$$(6,10)=2\cdot(3,5)=2\cdot(3,5-2\cdot3)=2\cdot(3,-1)=2,$$

$$(2,15)=(2,15-2\cdot7)=(2,1)=1.$$

由以上三式得 $(6,10,-15)=1$。

由定理8和9容易证明（留给读者）：

$$(a_1,a_2)(b_1,b_2)=(a_1b_1,a_1b_2,a_2b_1,a_2b_2),$$

以及一般地

$$(a_1,\cdots,a_r)(b_1,\cdots,b_s)=(a_1b_1,\cdots,a_1b_s,\cdots,a_rb_1,\cdots,a_rb_s).$$

定理10 设 $(m,a)=1$，则有 $(m,ab)=(m,b)$。

证 $m=0$ 时 $a=\pm1$，结论显然成立。$m\neq0$时，由定理1，定理8和定理9可得

① 我们约定 $(a)=|a|$。

$$(m,b)=(m,b(m,a))=(m,(mb,ab))$$
$$=(m,mb,ab)$$
$$=(m,ab).$$

这就证明了所要的结论。

定理11 设$(m,a)=1$。那么，若 $m|ab$，则 $m|b$。

证 由定理1及定理10得$|m|=(m,ab)=(m,b)$，这就推出$m|b$。

定理10和定理11是经常用到的。例如，当m是奇数时，由定理10推出$(m,2^kb)=(m,b)$，而由定理11推出：若$m|2^kb$，则$m|b$。

定理11常用形式是：若$(m_1,m_2)=1$，$m_1|n$，$m_2|n$，则$m_1m_2|n$。这因为由$m_1|n$知$n=m_1n_1$，由此利用条件$(m_2,m_1)=1$，从定理11推出$m_2|n_1$，因而$m_1m_2|n$。一般地可证明以下结论(留给读者)：若$m_1,\cdots,m_k$两两既约，及$m_j|n(1\leqslant j\leqslant k)$，则$m_1\cdots m_k|n$。

定理12 $[a_1,a_2](a_1,a_2)=|a_1a_2|$。

证 先假定$(a_1,a_2)=1$。设$L=[a_1,a_2]$。由定理6知$L|a_1a_2$。另一方面，由$a_1|L$知$L=a_1L'$。进而由$a_2|L=a_1L'$及$(a_2,a_1)=1$，由定理11知$a_2|L'$。所以$|a_1a_2||L$。这样，由§2定理1(v)知$L=|a_1a_2|$。所以结论成立。当$(a_1,a_2)\neq 1$时，由式(5)知$(a_1/(a_1,a_2),a_2/(a_1,a_2))=1$，所以由已证结论知

$$\left[\frac{a_1}{(a_1,a_2)},\ \frac{a_2}{(a_1,a_2)}\right]=\frac{|a_1a_2|}{(a_1,a_2)^2}.$$

由此及定理5$(k=2,m=(a_1,a_2))$即得所要结论。

定理12刻画了最大公约数与最小公倍数之间的关系。我们可以通过求出最大公约数来求得最小公倍数。

以上我们建立了最大公约数与最小公倍数理论，这些结论都是直接从定义出发来证明的。这种论证的方法与技巧在整除理论中是十分基本和重要的。

下面来举几个例子。

例 3 设 p 是素数。证明：

(i) $p\left|\binom{p}{j}\right.$, $1\leqslant j\leqslant p-1$，这里 $\binom{p}{j}$ 表组合数；

(ii) 对任意正整数 a, $p\mid a^p-a$；

(iii) 若 $(a,p)=1$，则 $p\mid a^{p-1}-1$。

证 已知组合数

$$\binom{p}{j}=\frac{p!}{j!(p-j)!}$$

是整数，即 $j!(p-j)!\mid p!$。由于 p 是素数，所以，对任意 $1\leqslant i\leqslant p-1$ 有 $(p,i)=1$。因此由定理10知

$$(p,j!(p-j)!)=1,\quad 1\leqslant j\leqslant p-1.$$

进而由定理 11 推出：当 $1\leqslant j\leqslant p-1$ 时 $j!(p-j)!\mid(p-1)!$，这就证明了(i).用归纳法来证(ii)。$a=1$时显然成立。假设 $a=n$ 时成立。当 $a=n+1$ 时，由(i)知

$$\begin{aligned}(n+1)^p-(n+1)&=n^p+\binom{p}{1}n^{p-1}+\cdots+\binom{p}{p-1}n\\&\quad+1-(n+1)\\&=n^p-n+p\cdot A,\end{aligned}$$

这里 A 为一整数。由此及假设知结论对 $a=n+1$ 也成立。这就证明了(ii)。应用定理11，由(ii)即推出(iii)。

例 4 证明：(i) $(a,uv)=(a,(a,u)v)$；

(ii) $(a,uv)\mid(a,u)(a,v)$。

证 由定理 1(i),(iii)，定理 9 及定理 8 即得

$$\begin{aligned}(a,uv)&=(a,uv,av)=(a,(uv,av))\\&=(a,(a,u)v).\end{aligned}$$

由定理 7 及定理 8 得

$$(a,(a,u)v)\mid((a,u)a,(a,u)v)=(a,u)(a,v).$$

由此及(i)即得(ii)。显见，(i)是定理10的推广。

例 5 设 k 是正整数。若一个有理数的 k 次方是整数，那么，这个有理数一定是整数。

证 不妨设这个有理数是 $b/a, a\geqslant 1, (a,b)=1$。若 $(b/a)^k=c$ 是整数，则 $ca^k=b^k$，所以 $a|b^k$。由于 $(a,b)=1$，所以由定理 11 知 $a|b$，因而 $1=(a,b)=a$。这就证明了所要的结果。

例 6 设 k 是正整数。证明：

(i) $(a^k,b^k)=(a,b)^k$。

(ii) 设 a,b 是正整数。若 $(a,b)=1$，$ab=c^k$，则 $a=(a,c)^k$，$b=(b,c)^k$。

证 由定理 8 得

$$(a^k,b^k)=(a,b)^k\left(\left(\frac{a}{(a,b)}\right)^k,\ \left(\frac{b}{(a,b)}\right)^k\right).$$

而由定理 3 知

$$\left(\frac{a}{(a,b)},\ \frac{b}{(a,b)}\right)=1.$$

由上式及定理10得

$$\left(\left(\frac{a}{(a,b)}\right)^k,\ \left(\frac{b}{(a,b)}\right)^k\right)=1.$$

由这及第一式就推出(i)。下面证(ii)。由定理 10 及 $(a,b)=1$ 知 $(a^{k-1},b)=1$。因而由定理 8 知，

$$a=a(a^{k-1},b)=(a^k,ab)=(a^k,c^k)=(a,c)^k,$$

最后一步用到了(i)。类似证 $b=(b,c)^k$。请读者解释(ii)的意义。

例 7 设 $a\geqslant 2, (a,b)=1$。证明：

(i) 存在正整数 $d\leqslant a-1$，使得 $a|b^d-1$。

(ii) 设 d_0 是满足(i)的最小正整数 d。那么，$a|b^h-1(h\geqslant 1)$ 的充要条件是 $d_0|h$。

证 由 $a\geqslant 2, (a,b)=1$ 知 $a\nmid b$，由此及 $(a,b)=1$，从定理1`推出 $a\nmid b^j, j\geqslant 1$。进而，由 § 3定理 1 知

$$b^j=q_ja+r_j,\quad 0\leqslant r_j<a.$$

这样，a 个余数 $r_0,r_1,\cdots,r_{a-1}$ 仅可能取 $a-1$ 个值，其中必有两个相等，设为 r_i,r_k。不妨设 $0\leqslant i<k<a$。因而有

$$a(q_k-q_i)=b^k-b^i=b^i(b^{k-i}-1).$$

由此从定理11推出 $a\mid b^{k-i}-1$，取 $d=k-i$ 即证明了(i)。(ii)的证明和§3例5(ii)的证明完全相同，只要把那里的 2 换为 b。

习　题　四（Ⅱ）

1．设 p 是素数，$(a,p^2)=p,(b,p^3)=p^2$。求 $(ab,p^4),(a+b,p^4)$。

2．设 p 是素数，$(a,b)=p$。求 $(a^2,b),(a^3,b),(a^2,b^3)$ 所可能取的值。

3．判断以下结论是否成立，对的给出证明，错的举出反例。

(i) 若 $(a,b)=(a,c)$，则 $[a,b]=[a,c]$。

(ii) 若 $(a,b)=(a,c)$，则 $(a,b,c)=(a,b)$。

(iii) 若 $d\mid a$，$d\mid a^2+b^2$，则 $d\mid b$。

(iv) 若 $a^4\mid b^3$，则 $a\mid b$。

(v) 若 $a^2\mid b^3$，则 $a\mid b$。

(vi) 若 $a^2\mid b^2$，则 $a\mid b$。

(vii) $ab\mid[a^2,b^2]$。

(viii) $[a^2,ab,b^2]=[a^2,b^2]$。

(ix) $(a^2,ab,b^2)=(a^2,b^2)$。

(x) $(a,b,c)=((a,b),(a,c))$。

(xi) 若 $d\mid a^2+1$，则 $d\mid a^4+1$。

(xii) 若 $d\mid a^2-1$，则 $d\mid a^4-1$。

4．证明 $\sqrt{2},\sqrt{3},\sqrt{15}$ 都不是有理数。

5．(i) 设整系数多项式 $P(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$，$a_0\neq0$。若 $P(x)$ 有有理根 x_0，则 x_0 必是整数，且 $x_0\mid a_0$。

(ii) 证明：x^5+3x^4+2x+1 没有有理根。

6. 设 $\theta=r\pi$，r 是有理数，证明：除了 $\cos\theta=0,\pm 1/2,\pm 1$ 外，$\cos\theta$ 一定是无理数，即除了 $\theta=k\pi, k\pi\pm\pi/3$，$k\pi+\pi/2$ 外，$\cos\theta$ 一定是无理数，k 为任意整数(提示：对任给正整数 n，必有首项系数为 1 的整系数多项式 $f_n(x)$，使 $2\cos n\alpha=f_n(2\cos\alpha)$，$\alpha$ 为任意实数)。

7. 设 n 是正整数，$n|ab$，$n\nmid a, n\nmid b$。再设 $a=d(a,ab/n)$。证明：$d|n, 1<d<n$。解释这题的意义。

8. 设 $(a,b)=1$。证明：

(i) $(d,ab)=(d,a)(d,b)$；

(ii) d 是 ab 的正除数的充要条件是 d 可表为 d_1d_2，这里 d_1 是 a 的正除数，d_2 是 b 的正除数，且这种表法唯一。

9. 证明：

$$[a_1,a_2,a_3,\cdots,a_n]=[[a_1,a_2],a_3,\cdots,a_n]$$
$$=[[a_1,\cdots,a_r],[a_{r+1},\cdots,a_n]].$$

10. 设 a,b,c 是正整数。证明：

(i) $[a,b,c](ab,bc,ca)=abc$。

(ii) $[a,b,c]=abc$ 的充要条件是 $(a,b)=(b,c)=(c,a)=1$。

11. 证明：$(a/(a,c),b/(b,a),c/(c,b))=1$。

12. 证明：$(a,b,c)(ab,bc,ca)=(a,b)(b,c)(c,a)$。

13. 证明：$(a,[b,c])=[(a,b),(a,c)]$。

14. 证明：$[a,(b,c)]=([a,b],[a,c])$。

15. 证明：(i) $([a,b],[b,c],[c,a])=[(a,b),(b,c),(c,a)]$。

(ii) $(a,b)(b,c)(c,a)[a,b,c]^2=[a,b][b,c][c,a](a,b,c)^2$。

16. 证明：

(i) 若 $(13,ab)=1$，则 $13|a^{12}-b^{12}$。

(ii) 若 $(91,ab)=1$，则 $91|a^{12}-b^{12}$。

(iii) 对任意的 n 有 $2730|n^{13}-n$。

17. 设 $p_1,\cdots,p_n$ 是 n 个两两不同的素数。再设 A_r 是其中任意取定的 r 个素数的乘积。证明：任一 $p_j(1\leqslant j\leqslant n)$ 都不能整除

$p_1\cdots p_n/A_r+A_r$。由此推出素数有无穷多个。

18. 设 p 是素数，$p\nmid a$。证明：对任给的正整数 k 有

(i) $\phi(p^k)=(p-1)p^{k-1}$，$\phi(n)$由§4习题四(Ⅰ)第19题给出；

(ii) $p^k\mid a^{\phi(p^k)}-1$。

19. 设 $p_1,\cdots,p_r$ 是两两不同的素数，$m=p_1^{k_1}\cdots p_r^{k_r}$，$k_j(1\leqslant j\leqslant r)$是正整数，以及 $\lambda(m)=[\phi(p_1^{k_1}),\cdots,\phi(p_r^{k_r})]=[p_1^{k_1-1}(p_1-1),\cdots,p_r^{k_r-1}(p_r-1)]$(见上题)。证明：当$(a,m)=1$时，有 $m\mid a^{\lambda(m)}-1$。这给出了§4 例 7(i)的另一证明，也证明了§3习题三第28题当$(a,m)=1$时结论就成立。

20. 设 $2\nmid a,k_0\geqslant3$。证明：$2^{k_0}\mid a^{2^{k_0-2}}-1$。进而推出：若 $m=2^{k_0}p_1^{k_1}\cdots p_r^{k_r}$，$p_1,\cdots,p_r$ 是两两不同的奇素数，$k_0\geqslant3,k_j\geqslant1(1\leqslant j\leqslant r)$，及$(a,m)=1$，则有 $m\mid a^{\lambda_1(m)}-1$，这里

$$\lambda_1(m)=\left[\frac{1}{2}\phi(2^{k_0}),\phi(p_1^{k_1}),\cdots,\phi(p_r^{k_r})\right]$$

$$=[2^{k_0-2},p_1^{k_1-1}(p_1-1),\cdots,p_r^{k_r-1}(p_r-1)].$$

21. 设 $m>1$。证明：$m\nmid 2^m-1$。

22. 设 $f(x)=a_nx^n+\cdots+a_0$，$g(x)=b_mx^m+\cdots+b_0$是整系数多项式，$h(x)=f(x)g(x)=c_{m+n}x^{m+n}+\cdots+c_0$。证明：

$$(a_n,\cdots,a_0)(b_m,\cdots,b_0)=(c_{m+n},\cdots,c_0).$$

23. 设 a,b,m 是正整数，$(a,b)=1$。证明：在算术数列 $a+kb(k=0,1,2,\cdots)$中，必有无穷多个数和m既约。

24. 设 $a>b>0,n>1$。证明：$a^n-b^n\nmid a^n+b^n$。

25. 设 $a>b\geqslant1,n>1$。证明：

$$((a^n-b^n)/(a-b),a-b)=(n(a,b)^{n-1},a-b).$$

26. (i) 若 $n\mid 2^n-2$，n 一定是素数吗？考虑 $n=341$。具有这种性质的数称为伪素数；

(ii) 若 $n\mid 2^n-2$，则 $m\mid 2^m-2$，这里 $m=2^n-1$；

(iii) 设 $n=161038$，验证 $n\mid 2^n-2$。

27. (i) 一个合数 n 称为是绝对伪素数，如果对任意整数 a

必有 $n|a^n-a$。证明：561是绝对伪素数，但341不是。

(ii) 设 $m\geqslant1$。若 $q_1=6m+1$，$q_2=12m+1$，$q_3=18m+1$ 均为素数，则 $n=q_1q_2q_3$ 是绝对伪素数。举出几个这样的 m。

28．证明：存在无穷多个 n 使 $n|2^n+1$。

29．证明：(i) 若 $n|2^n+2$，$n-1|2^n+1$，则 $m|2^m+2$，$m-1|2^m+1$，这里 $m=2^n+2$；

(ii) 存在无穷多个 n 使 $n|2^n+2$。

30．证明：存在无穷多个合数 n，使对任意整数 a 有

$$n|a^{n-1}-a。$$

对于最大公约数我们至今还没有给出一个明确的表示形式。下面来讨论这一点。

定理13 设 $a_1,\cdots,a_k$ 是不全为零的整数。我们有

(i)

$$(a_1,\cdots,a_k)=\min\{s=a_1x_1+\cdots+a_kx_k:x_j\in\mathbf{Z}(1\leqslant j\leqslant k),s>0\},$$

即 $a_1,\cdots,a_k$ 的最大公约数等于 $a_1,\cdots,a_k$ 的所有整系数线性组合组成的集合 S 中的最小正整数。

(ii) 一定存在一组整数 $x_{1,0},\cdots,x_{k,0}$ 使得

$$(a_1,\cdots,a_k)=a_1x_{1,0}+\cdots+a_kx_{k,0}。\tag{11}$$

证　由于 $0<a_1^2+\cdots+a_k^2\in S$，所以集合 S 中有正整数，由最小自然数原理知 S 中必有最小正整数，设为 s_0。显见，对任一公约数 $d|a_j(1\leqslant j\leqslant k)$ 必有 $d|s_0$，所以 $|d|\leqslant s_0$。另一方面，对任一 a_j 由带余数除法知

$$a_j=q_js_0+r_j,\qquad 0\leqslant r_j<s_0。$$

显见 $r_j\in S$。若 $r_j>0$，则和 s_0 的最小性矛盾，所以，$r_j=0$，即 $s_0|a_j(1\leqslant j\leqslant k)$。所以，$s_0$ 是最大公约数。s_0 当然是式（11）右边的形式。证毕。

最大公约数能表为式（11）的形式这一结论是十分重要的（虽然这里只是说 $x_{1,0},\cdots,x_{k,0}$ 存在并没有指出如何求 $x_{1,0},\cdots,x_{k,0}$，而且显然不是唯一的），因为这使得我们在论证它们的性质的过程中有了一个便于推导的表示式，而用不着总是从定义出发，需要较高的技巧。为了说明这一点，下面我们利用定理13来重新给出定理 7 —定理11的证明①。

定理7的证明 显见，只要证必要性。(i) 由定义知成立，而(ii)由表示式（11）直接看出（事实上，在定理13的证明中，是先指出 s_0 满足条件(i)和(ii)）。

定理8的证明 由定理13知，可设

$$(b_1,\cdots,b_k)=b_1y_1+\cdots+b_ky_k,$$

$$(mb_1,\cdots,mb_k)=(mb_1)x_1+\cdots+(mb_k)x_k.$$

这样，根据这两式，由 $m(b_1\cdots,b_k)\mid mb_j\ (1\leqslant j\leqslant k)$ 推出

$$m(b_1,\cdots,b_k)\mid(mb_1,\cdots,mb_k);$$

由 $(mb_1,\cdots,mb_k)\mid mb_j\ (1\leqslant j\leqslant k)$，推出

$$(mb_1,\cdots,mb_k)\mid(mb_1)y_1+\cdots+(mb_k)y_k=m(b_1,\cdots,b_k).$$

由以上两式就证明了所要结论。

定理9的证明 先证(i)。由定理13知，可设

$$D_1=(a_1,\cdots,a_k)=a_1x_1+\cdots+a_kx_k,$$

$$D_2=(a_1,a_2)=a_1y_1+a_2y_2,$$

$$D_3=((a_1,a_2),a_3,\cdots,a_k)=(a_1,a_2)z_2+a_3z_3+\cdots+a_kz_k.$$

由 $D_3\mid(a_1,a_2),D_3\mid a_j\ (3\leqslant j\leqslant k)$ 知 $D_3\mid a_j\ (1\leqslant j\leqslant k)$，所以 $D_3\mid D_1$。注意到

$$D_3=a_1(y_1z_2)+a_2(y_2z_2)+a_3z_3+\cdots+a_kz_k,$$

及 $D_1\mid a_j\ (1\leqslant j\leqslant k)$，就推出 $D_1\mid D_3$。所以 $D_1=D_3$。同样的方法可证(ii)，具体推导留给读者。

定理10的证明 由定理13知，可设

① 原来的证明是在定理 6 的基础上，先证明定理 7 ，然后依此证明各定理．而定理 6 是关于最小公倍数的性质．这里将给出的证明和最小公倍数的概念无关。

$$(m,b)=mx_1+bx_2,$$
$$(m,ab)=my_1+(ab)y_2.$$
由$(m,b)|m$,$(m,b)|b$及第二式就推出$(m,b)|(m,ab)$。由条件知，存在z_1,z_2使
$$mz_1+az_2=1. \qquad (12)$$
因而有
$$(m,b)=(mx_1+bx_2)(mz_1+az_2)$$
$$=m(mx_1z_1+ax_1z_2+bx_2z_1)+(ab)(x_2z_2).$$
由此及$(m,ab)|m$,$(m,ab)|ab$就推出$(m,ab)|(m,b)$。这就证明了定理。

定理11的证明 由定理13及条件知有式（12）成立。所以，有$m(bz_1)+(ab)z_2=b$。由此及$m|ab$即得$m|b$。

应该指出的是：在上述定理7—定理11的证明中，除了整除最基本的性质（§2定理1）之外，都只用了定理13而不需要其它结论。

例 8 若$(a,b)=1$，则任一整数n必可表为
$$n=ax+by, \qquad x,y\text{是整数}.$$

由$(a,b)=1$及定理13知，存在x_0,y_0使$ax_0+by_0=1$。因而，取$x=nx_0$,$y=ny_0$即满足要求。

例 9 设a,b是整数，$11\nmid a$。证明：$11\nmid a^2+5b^2$。

证 用反证法。若$11|a^2+5b^2$，则由$11\nmid a$推出$11\nmid b$。因此由定理13知，必有x,y使
$$11x+by=1.$$
由此及$11|y^2(a^2+5b^2)=(ay)^2+5(by)^2$推出
$$11|(ay)^2+5.$$
但对所有的y,$(ay)^2$被11除后所得的余数必在0,1,4,9,5,3中，所以上式不可能成立。因此，必有$11\nmid a^2+5b^2$。以上讨论也表明：$11|a^2+5b^2$的充要条件是$11|a$,$11|b$。

本题也可以用下面的方法直接证明：x^2被11除后所得的余数

必在0,1,4,9,5,3中。容易直接验证，当r,s取值0,1,4,9,5,3，且不同时为零时，必均有

$$11 \nmid r^2+5s^2.$$

由此即推出所要结论。但这个方法所需作的直接验算比上面的方法要多一倍以上。

例10 设n,k是正整数，$(k,n)=1,0<k<n$。再设集合$M=\{1,2,\cdots,n-1\}$。现对集合M中的每个数i涂上蓝色或白色，要满足以下条件：(i) i和$n-i$要涂上同一种颜色；(ii) 当$i\neq k$时，i和$|k-i|$要涂上同一种颜色。证明：所有的数一定都涂上同一种颜色。

证 我们来证明：所有的$i\in M$必和k同色。由例8知存在x,y使

$$i=xk+yn.$$

由$1\leqslant i\leqslant n-1$知，$x,y$的取值可能出现三种情形：(a) $x>0$，$y=0$；(b) $x>0,y<0$；(c) $x<0,y>0$。

在情形(a)，由条件(ii)知i和k同色。

在情形(c)，由条件(i)知i和$n-i=(-x)k+(-y+1)n$同色。若$-y+1=0$这就变为情形(a)，若$-y+1<0$这就变为(b)。所以只要讨论情形(b)。

在情形(b)必有$x>-y$。这时又可分三种情形：(Ⅰ) $k=i$；(Ⅱ) $k>i$；(Ⅲ) $k<i$。当(Ⅰ)出现时结论成立。当(Ⅲ)出现时，由带余数除法知：

$$i=qk+i',\quad 0\leqslant i'<k.$$

若$i'=0$，变为情形(a)，结论成立。若$1\leqslant i'<k$，由条件(ii)知，i和$i'=i-qk=(x-q)k+yn$同色，代替i考虑i'就变为情形(Ⅱ)。当(Ⅱ)出现时，由条件(ii)知，i和$k-i=(-x+1)k-yn$同色，再由条件(i)知i和$i''=n-(k-i)=(x-1)k+(y+1)n$同色。若$y+1=0$则结论成立，若$y+1<0$，则又变为情形(b)，继续对$i''$分(Ⅰ),(Ⅱ),(Ⅲ)三种情形考虑。这样，讨论若干步

后，总可得到 i 和 $x'k$ 即 k 同色。证毕。

定理 13 仅指出了 $x_{1,0},\cdots,x_{k,0}$的存在性。下一节将讨论如何求$x_{1,0},\cdots,x_{k,0}$的算法。

习 题 四（Ⅲ）

1．证明：从定理13的(ii)成立可推出定理13的(i)成立。

2．设 n,a,b,c是正整数，$(b,c)=1$。证明：若$c\mid n!$，则

$$c\mid a(a+b)(a+2b)\cdots(a+(n-1)b)。$$

3．设$a_1<a_2<a_3<\cdots$是一个无穷正整数列。证明：在这个数列中一定存在两个数a_s,a_t，使得有无穷多个a_n可表为$a_n=xa_s+ya_t$，x,y是整数。

4．§4 例10中，当$(n,k)=d>1$时，若按条件（i），(ii)对集合M中的每个数涂一种颜色，问M中的数最多可涂上几种颜色.

5．证明：$13\mid a^2-7b^2$ 的充要条件是$13\mid a,13\mid b$。

6．设$1\leqslant a<b$，a,b 既约。证明：

(i) 既约分数 a/b 是十进位的纯循环小数的充要条件是$(b,10)=1$；

(ii) 若 a/b 是纯循环小数，最小的循环节为 t_0(即$a/b=0.d_1\cdots d_{t_0}d_1\cdots d_{t_0}\cdots$是十进位纯循环小数表示，而对比 t_0 小的正整数t，a/b 不可能表为循环节为 t 的纯循环小数)，则 t_0恰好是使$b\mid 10^d-1$ 成立的最小正整数 d。

7．设$1\leqslant a<b,a,b$既约。证明

(i) b 可唯一地表为$2^\alpha5^\beta b_1,(b_1,10)=1$；

(ii) 当$\alpha=\beta=0$时，a/b 是纯循环小数，即上题所讨论的情形；

(iii)当$b_1=1$时，a/b 是有限小数；

(iv) 当 $\gamma=\max(\alpha,\beta)>0,b_1>1$ 时，a/b是混循环小数，即$a/b=0.c_1\cdots c_{s_0}d_1\cdots d_{t_0}d_1\cdots d_{t_0}\cdots$，最小的不循环位数 $s_0=\gamma$，最小的循环节 t_0 等于使 $b_1\mid 10^d-1$ 成立的最小正整数d。

§5 辗转相除法

辗转相除法也叫作 Euclid 算法，它是指下面的算法：

定理1 设 u_0,u_1 是给定的两个整数，$u_1\neq 0$，$u_1\nmid u_0$。我们一定可以重复应用§3定理1得到下面$k+1$个等式：

$$
\begin{array}{ll}
u_0=q_0u_1+u_2, & 0<u_2<|u_1|,\\
u_1=q_1u_2+u_3, & 0<u_3<u_2,\\
u_2=q_2u_3+u_4, & 0<u_4<u_3,\\
\cdots\cdots & \cdots\cdots\\
u_{k-2}=q_{k-2}u_{k-1}+u_k, & 0<u_k<u_{k-1},\\
u_{k-1}=q_{k-1}u_k+u_{k+1}, & 0<u_{k+1}<u_k,\\
u_k=q_ku_{k+1}. &
\end{array}
\tag{1}
$$

证 对 u_0,u_1 应用§3定理1，由 $u_1\nmid u_0$ 知必有第一式成立。同样的，如果 $u_2\nmid u_1$ 就得到第二式。如果 $u_2|u_1$ 就证明定理对 $k=1$ 成立。依此这样作，就得到

$$|u_1|>u_2>u_3>\cdots>u_{j+1}>0$$

及前面 j 个等式成立。若 $u_{j+1}|u_j$，则定理对 $k=j$ 成立；若 $u_{j+1}\nmid u_j$，则继续对 u_j,u_{j+1} 用§3定理1。由于小于 $|u_1|$ 的正整数只有有限个以及1整除任一整数，所以这过程不能无限制地做下去，一定会出现某个k，要么$1<u_{k+1}|u_k$，要么 $1=u_{k+1}|u_k$。证毕。

由定理1立即推出

定理2 在定理1的条件和符号下，我们有

(i) $$u_{k+1}=(u_0,u_1); \tag{2}$$

(ii) $d|u_0$ 且 $d|u_1$ 的充要条件是 $d|u_{k+1}$；

(iii) 存在整数 x_0,x_1 使

$$u_{k+1}=x_0u_0+x_1u_1. \tag{3}$$

证 利用§4定理1的 (i) 和 (iv)，从式 (1) 的最后一式

开始，依次往上推，可得

$$u_{k+1}=(u_{k+1},u_k)=(u_k,u_{k-1})=(u_{k-1},u_{k-2})=\cdots$$
$$=(u_4,u_3)=(u_3,u_2)=(u_2,u_1)=(u_1,u_0), \qquad (4)$$

这就证明了（i）。利用§2定理1的（ii）和（iii），从式（1）立即推出（ii）。由式（1）的第 k 式知 u_{k+1} 可表成 u_{k-1} 和 u_k 的整系数线性组合，利用式(1)的第 $k-1$ 式可消去这个整系数线性表示式中的 u_k，得到 u_{k+1} 表为 u_{k-2} 和 u_{k-1} 的整系数线性组合。这样，依此利用式（1）的第 $k-2,k-3,\cdots,2,1$ 式，就可相应地消去 $u_{k-1},u_{k-2},\cdots,u_3,u_2$，最后得到 u_{k+1} 表为 u_0 和 u_1 的整系数线性组合，这就证明了（iii）。证毕。

显见，当 $u_1|u_0$ 时，定理2也成立。定理2表明：（i）辗转相除法（定理1）给出了求两个数的最大公约数的一个十分方便的具体算法；（ii）利用辗转相除法直接证明了§4定理7($k=2$ 的情形)；（iii）利用辗转相除法不但直接证明了§4定理13的(ii)($k=2$ 的情形)，而且同时给出了计算 x_0,x_1 的具体算法。我们再注意到由§4定理7($k=2$) 可推出§4定理9的（i）（见那里的证明），而由§4定理9(i) 利用归纳法就可证明§4定理7对任意 k 都成立，以及§4定理13的（ii）对任意 k 都成立(请读者自证)。这样，§4所建立的理论全部可以直接在定理2，即辗转相除法的基础上建立起来。

例1 求198和252的最大公约数，并把它表为198和252的整系数线性组合。

$252=1\cdot198+54$	$18=-198+4(252-198)$
$198=3\cdot54+36$	$=4\cdot252-5\cdot198$
$54=1\cdot36+18$	$18=54-(198-3\cdot54)$
$36=2\cdot18$ ↓	$=-198+4\cdot54$
	$18=54-36$ ↑

$$(252,198)=(198,54)=(54,36)=(36,18)=18.$$

例2 求198，252，924的最大公约数，并把它表为198，252和

924的整系数线性组合。

由§4定理9(i) 及例1知

$$(198,252,924)=((198,252),924)=(18,924).$$

$$924=51\cdot 18+6 \quad \Big| \quad 6=924-51\cdot 18$$
$$18=3\cdot 6$$

由此及例1得：$(198,252,924)=6$。

$$6=924-51\cdot 18=924-51(4\cdot 252-5\cdot 198)$$
$$=924-204\cdot 252+255\cdot 198.$$

例3 设 m,n 是正整数。证明

$$(2^m-1,2^n-1)=2^{(m,n)}-1.$$

证 不妨设$m\geqslant n$。由带余数除法得

$$m=q_1n+r_1,\qquad 0\leqslant r_1<n.$$

我们有

$$2^m-1=2^{q_1n+r_1}-2^{r_1}+2^{r_1}-1=2^{r_1}(2^{q_1n}-1)+2^{r_1}-1.$$

由此及$2^n-1|2^{q_1n}-1$得

$$(2^m-1,2^n-1)=(2^n-1,2^{r_1}-1).$$

注意到$(m,n)=(n,r_1)$，若 $r_1=0$，则$(m,n)=n$，结论成立。若$r_1>0$，则继续对$(2^n-1,2^{r_1}-1)$作同样的讨论，由辗转相除法知，结论成立。显见，2用任一大于1的自然数 a 代替，结论都成立。

习 题 五

1．用§5定理1的辗转相除法求以下数组的最大公约数，并把它表为这些数的整系数线性组合：

(i) 1819, 3587；(ii) 2947, 3997；(iii) −1109, 4999；

(iv) 15, 21, −35；(v) 210, −330, 1155。

2．设 $a>b$, $(a,b)=1$。证明：

$$(a^m-b^m,a^n-b^n)=a^{(m,n)}-b^{(m,n)}.$$

3．设 v_0,v_1 是给定的两个整数，$v_1\neq 0$, $v_1\nmid v_0$。我们一定可

以重复应用§3式(3″)形式的带余数除法得到下面$h+1$个等式：

$$v_0=q_0v_1+v_2,\qquad -|v_1|/2\leqslant v_2<|v_1|/2,\ v_2\neq 0,$$
$$v_1=q_1v_2+v_3,\qquad -|v_2|/2\leqslant v_3<|v_2|/2,\ v_3\neq 0,$$
$$v_2=q_2v_3+v_4,\qquad -|v_3|/2\leqslant v_4<|v_3|/2,\ v_4\neq 0,$$
$$\cdots\cdots\qquad\cdots\cdots$$
$$v_{h-2}=q_{h-2}v_{h-1}+v_h,\qquad -|v_{h-1}|/2\leqslant v_h<|v_{h-1}|/2,\ v_h\neq 0,$$
$$u_{h-1}=q_{h-1}v_h+v_{h+1},\qquad -|v_h|/2\leqslant v_{h+1}<|v_h|/2,\ v_{h+1}\neq 0,$$
$$v_h=q_hv_{h+1}.$$

这种算法也称为辗转相除法或Euclid 除法。

4．在第 3 题的条件和符号下，证明：

(i) $|v_{h+1}|=(v_0,v_1)$；

(ii) $d|v_0$且$d|v_1$的充要条件是$d|v_{h+1}$；

(iii) 存在整数x_0,x_1使得$v_{h+1}=x_0v_0+x_1v_1$。

5．利用第 3 题给出的辗转相除法来做第 1 题的 (i)，(ii)，及 (iii)。比较用这两种辗转相除法来做这三个小题时，所做的带余数除法的次数$k+1$和$h+1$的大小。

6．在§5定理 1 的条件和符号下，令

$$P_{-1}=1,P_0=q_0,\ P_j=q_jP_{j-1}+P_{j-2},\qquad Q_{-1}=0,Q_0=1,\ Q_j=q_jQ_{j-1}+Q_{j-2},\qquad j=1,2,\cdots,k-1.$$

那么，我们有

$$(-1)^ju_j=Q_{j-2}u_0-P_{j-2}u_1,\qquad j=1,2,\cdots,k+1.$$

7．用相应于第 3 题的辗转相除法来推出类似于第 6 题的结论。

8．设§5定理 1 中的$u_0>u_1>1$。再设$b_0=1,b_1=2$，及$b_{j+1}=b_j+b_{j-1},j=1,2,\cdots$。那么，在§5定理 1 的符号下有 $u_1\geqslant b_k$。进而证明：$k+1\leqslant 2(\log u_1)/\log 2$。试解释这结果的意义。

9．在第 3 题中设$v_0>v_1>1$。再设 $c_0=1,c_1=2$及$c_{j+1}=2c_j+c_{j-1},j=1,2,\cdots$。那么有$v_1\geqslant c_h$。进而证明：

(i) $h\leqslant(\log v_1)/\log 2$；

(ii) 当$v_1 \geqslant 32$时，$h+1 \leqslant (\log v_1)/\log 2$。

10．设$a>b>1$。设k是在§5定理1中取$u_0=a, u_1=b$时所得到的，h是在第3题中取$v_0=a, v_1=b$时所得到的。证明必有$h \leqslant k$。

11．设p是奇素数，q是2^p-1的素因数。证明$q=2kp+1$。

12．利用上题求$2^{11}-1, 2^{23}-1$的素因数分解式。

13．当p为素数时，$M_p=2^p-1$形式的数称为Mersenne数。把这种数用二进位来表示，利用§5定理1的辗转相除法（出现的数均用二进位表示）来直接证明：所有的Mersenne数两两互素。

§6 算术基本定理(A)

现在，我们利用§4的结果来证明算术基本定理，即§2定理5中的表示式（1）是唯一的（不计次序）。先来证明：

定理1 设p是素数，$p|a_1a_2$。那么，$p|a_1$或$p|a_2$至少有一个成立。一般地，若$p|a_1\cdots a_k$，则$p|a_1, \cdots, p|a_k$至少有一个成立。

证 若$p\nmid a_1$，则由§4定理1(v)知，$(p, a_1)=1$。由此及$p|a_1a_2$，从§4定理11就推出$p|a_2$。对一般情形的证明留给读者。

定理2(**算术基本定理**) 设$a>1$，那么，必有

$$a=p_1p_2\cdots p_s, \tag{1}$$

其中$p_j(1 \leqslant j \leqslant s)$是素数，且在不计次序的意义下，表示式（1）是唯一的。

证 由§2定理5知，表示式(1)一定存在。下面来证唯一性。不妨设$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_s$。若还有表示式

$$a=q_1q_2\cdots q_r, \qquad q_1 \leqslant q_2 \cdots \leqslant q_r,$$

$q_i(1 \leqslant i \leqslant r)$是素数，我们来证明必有$r=s, p_j=q_j(1 \leqslant j \leqslant s)$。不妨设$r \geqslant s$。利用定理1，由$q_1|a=p_1p_2\cdots p_s$知，必有某个$p_j$满足$q_1|p_j$。由于$q_1$和$p_j$是素数，所以$q_1=p_j$。同样，利用定理1，

由$p_1|a=q_1q_2\cdots q_r$知，必有某个q_i满足$p_1|q_i$，因而$p_1=q_i$。由于$q_1\leqslant q_i=p_1\leqslant p_j$，所以$p_1=q_1$。这样，就有

$$q_2q_3\cdots q_r=p_2p_3\cdots p_s.$$

由同样的论证，依次可得$q_2=p_2,\cdots,q_s=p_s$，

$$q_{s+1}\cdots q_r=1.$$

上式是不可能的，除非$r=s$，即不存在$q_{s+1},\cdots,q_r$。证毕。

把式(1)中相同的素数合并，即得

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\qquad p_1<p_2<\cdots<p_s \tag{2}$$

（这里的p_j和式（1）中的不表示相同的素数）。式（2）称为是a的标准素因数分解式。

推论3　设a由式（2）给出。那么，d是a的正除数的充要条件是

$$d=p_1^{e_1}\cdots p_s^{e_s},\qquad 0\leqslant e_j\leqslant \alpha_j,\ 1\leqslant j\leqslant s. \tag{3}$$

证　充分性是显然的。下证必要性。当$d=1$时，$e_j=0(1\leqslant j\leqslant s)$，结论当然成立。若$d>1$，则由$d|a$及定理1知$d$的素除数必在$p_1,\cdots,p_s$中，所以$d$的标准分解式必为

$$d=p_1^{e_1}\cdots p_s^{e_s},\qquad 0\leqslant e_j,\ 1\leqslant j\leqslant s.$$

我们来证明必有$e_j\leqslant\alpha_j(1\leqslant j\leqslant s)$。只要证$e_1\leqslant\alpha_1$，其它相同。若$e_1>\alpha_1$，则由此及$d|a$推出

$$p_1^{e_1-\alpha_1}p_2^{e_2}\cdots p_s^{e_s}|p_2^{\alpha_2}\cdots p_s^{\alpha_s},$$

因此，$p_1|p_2^{\alpha_2}\cdots p_s^{\alpha_s}$。由此及定理1推出$p_1$必和$p_2,\cdots,p_s$之一相等，矛盾。

推论4　设a由式（2）给出，

$$b=p_1^{\beta_1}\cdots p_s^{\beta_s},$$

这里允许某个α_j或β_j为零。那么

$$(a,b)=p_1^{\delta_1}\cdots p_s^{\delta_s},\quad \delta_j=\min(\alpha_j,\beta_j),\ 1\leqslant j\leqslant s, \tag{4}$$

$$[a,b]=p_1^{\gamma_1}\cdots p_s^{\gamma_s},\quad \gamma_j=\max(\alpha_j,\beta_j),\ 1\leqslant j\leqslant s, \tag{5}$$

以及

$$(a,b)[a,b]=ab. \tag{6}$$

推论 4 可由推论 3 直接推出。详细论证留给读者。

下面是一个经常有用的结论①。

推论5 若$(a,b)=1$，$ab=c^k$，则

$$a=u^k,\quad b=v^k.$$

证 设$c=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则

$$c^k=p_1^{k\alpha_1}\cdots p_s^{k\alpha_s}.$$

由推论 4 知，可设

$$a=p_1^{\beta_1}\cdots p_s^{\beta_s},\quad b=p_1^{\gamma_1}\cdots p_s^{\gamma_s}.$$

由条件$ab=c^k$知，$\beta_j+\gamma_j=k\alpha_j$ $(1\leqslant j\leqslant s)$。而由$(a,b)=1$知$\min(\beta_j,\gamma_j)=0(1\leqslant j\leqslant s)$。由以上两式立即得到：必有

$$\beta_j=0,\gamma_j=k\alpha_j\ \text{或}\ \beta_j=k\alpha_j,\gamma_j=0.$$

这就证明了所要结论。显见，$u=(a,c)$，$v=(b,c)$。

我们说过对一个整数的约数知道得很少。推论 3 表明：只要知道了正整数$a>1$的标准分解式(2)，它的所有的正约数就全知道了，且由式(3)给出。这一点具有重要的理论和应用价值。

推论6 设a是正整数，$\tau(a)$表示a的所有正除数的个数(通常称为除数函数)。若a有标准素因数分解式(2)，则

$$\tau(a)=(\alpha_1+1)\cdots(\alpha_s+1)=\tau(p_1^{\alpha_1})\cdots\tau(p_s^{\alpha_s}).\tag{7}$$

这由推论 3 直接推出。显见，$\tau(1)=1$，这可看作$\alpha_1=\cdots=\alpha_s=0$的情形，即式(7)对$a=1$也成立。

推论7 设a是正整数，$\sigma(a)$表示a的所有正除数之和。那么，$\sigma(1)=1$，当a有标准素因数分解式(2)时，

$$\begin{aligned}\sigma(a)&=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}=\prod_{j=1}^{s}\frac{p_j^{\alpha_j+1}-1}{p_j-1}\\&=\sigma(p_1^{\alpha_1})\cdots\sigma(p_s^{\alpha_s}).\end{aligned}\tag{8}$$

为了把证明叙述得更清楚，先引进几个有关求和与求积的符号，这在数学中是经常用到的。

---

① 这结论已在§4例6 (ii) 中证明，但那个证明技巧性强。

设 h 是给定的整数，k是给定的正整数。再设 z_i 是依赖于参数$i(h+1\leqslant i\leqslant h+k)$的$k$个复数。我们记这 k 个复数的和为

$$\sum_{i=h+1}^{h+k} z_i = z_{h+1}+\cdots+z_{h+k}; \tag{9}$$

它们的积为

$$\prod_{i=h+1}^{h+k} z_i = z_{h+1}\cdot\cdots\cdot z_{h+k}. \tag{10}$$

一般地，设$h_1,\cdots,h_r$ 是给定的整数，$k_1,\cdots,k_r$是给定的正整数。再设$z_{i_1,\cdots,i_r}$是依赖于参数$i_1(h_1+1\leqslant i_1\leqslant h_1+k_1),\cdots,i_r(h_r+1\leqslant i_r\leqslant h_r+k_r)$的 $k_1\cdots k_r$ 个复数。我们以多重求和号

$$\sum_{\substack{h_j+1\leqslant i_j\leqslant h_j+k_j\\ 1\leqslant j\leqslant r}} z_{i_1,\cdots,i_r} \tag{11}$$

表示这$k_1\cdots k_r$个复数之和；以多重求积号

$$\prod_{\substack{h_j+1\leqslant i_j\leqslant h_j+k_j\\ 1\leqslant j\leqslant r}} z_{i_1,\cdots,i_r} \tag{12}$$

表示这些复数之积。根据加法的交换律与结合律，多重和式(11)可表为累次求和：

$$\sum_{\substack{h_j+1\leqslant i_j\leqslant h_j+k_j\\ 1\leqslant j\leqslant r}} z_{i_1,\cdots,i_r} = \sum_{i_1=h_1+1}^{h_1+k_1}\cdots\sum_{i_{r-1}=h_{r-1}+1}^{h_{r-1}+k_{r-1}}\ \sum_{i_r=h_r+1}^{h_r+k_r} z_{i_1,\cdots,i_{r-1},i_r}, \tag{13}$$

上式右边的累次求和式是表示：对固定的 $i_1,\cdots,i_{r-1}$，先对参数 i_r $(h_r+1\leqslant i_r\leqslant h_r+k_r)$给出的$k_r$ 个复数$z_{i_1,\cdots,i_{r-1},i_r}$ 求和得到$z^{(1)}_{i_1,\cdots,i_{r-1}}$，这是依赖于参数$i_1(h_1+1\leqslant i_1\leqslant h_1+k_1),\cdots,i_{r-1}(h_{r-1}+1\leqslant i_{r-1}\leqslant h_{r-1}+k_{r-1})$的复数；再固定$i_1,\cdots,i_{r-2}$，先对参数$i_{r-1}(h_{r-1}+1\leqslant i_{r-1}\leqslant h_{r-1}+k_{r-1})$给出的$k_{r-1}$个复数 $z^{(1)}_{i_1,\cdots,i_{r-1}}$ 求和得到$z^{(2)}_{i_1,\cdots,i_{r-2}}$，等等，通过这样的求和次序来求出多重和

式(11)。通常，把这种累次求和称为是先对参数 i_r 求和，再对 i_{r-1} 求和，…，最后对参数 i_1 求和。显然，由加法的交换律和结合律知，这种对参数 $i_1,\cdots,i_r$ 的累次求和的次序可以任意选定。同样，根据乘法的交换律与结合律，多重乘积(12)可表为累次求积

$$\prod_{\substack{h_j+1\leqslant i_j\leqslant h_j+k_j\\1\leqslant j\leqslant r}} z_{i_1,\cdots,i_r} = \prod_{i_1=h_1+1}^{h_1+k_1}\cdots\prod_{i_{r-1}=h_{r-1}+1}^{h_{r-1}+k_{r-1}}\prod_{i_r=h_r+1}^{h_r+k_r} z_{i_1,\cdots,i_{r-1},i_r}, \tag{14}$$

累次求积的意义和累次求和完全一样。

设$f(n)$是定义在全体正整数集合上的复值函数，a 是给定的正整数。在数论中经常用以下的符号：

$$\sum_{d\mid a} f(d) = \text{函数 } f \text{ 在 } a \text{ 的所有不同的正除数上的值之和；} \tag{15}$$

$$\sum_{p\mid a} f(p) = \text{函数 } f \text{ 在 } a \text{ 的所有不同的素除数上的值之和①；} \tag{16}$$

$$\prod_{d\mid a} f(d) = \text{函数 } f \text{ 在 } a \text{ 的所有不同的正除数上的值之积；} \tag{17}$$

$$\prod_{p\mid a} f(p) = \text{函数 } f \text{ 在 } a \text{ 的所有不同的素除数上的值之积②．} \tag{18}$$

这样，取$f(n)\equiv 1$就有

$$\tau(a) = \sum_{d\mid a} 1. \tag{19}$$

① 约定$a=1$时为零。

② 约定$a=1$时为 1。

取 $f(n)=n$ 就有

$$\sigma(a)=\sum_{d\mid a}d. \tag{20}$$

引理8 设 $f(n)$ 是定义在正整数集合上的复值函数，正整数 a 由式(2)给出。那么

$$\sum_{d\mid a}f(d)=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_s=0}^{\alpha_s}f(p_1^{e_1}\cdots p_s^{e_s}), \tag{21}$$

$$\prod_{d\mid a}f(d)=\prod_{e_1=0}^{\alpha_1}\cdots\prod_{e_s=0}^{\alpha_s}f(p_1^{e_1}\cdots p_s^{e_s}). \tag{22}$$

证 由式(15)给出的定义及推论3知，$\sum\limits_{d\mid a}f(d)$就是下面这组由参数$e_1,\cdots,e_s$给出复数之和：

$$\begin{cases}z_{e_1,\cdots,e_s}=f(p_1^{e_1}\cdots p_s^{e_s}),\\(-1)+1=0\leqslant e_j\leqslant\alpha_j=(-1)+\alpha_j+1,\ 1\leqslant j\leqslant s,\end{cases}$$

即在式(11)中取 $h_j=-1$，$k_j=\alpha_j+1(1\leqslant j\leqslant s)$。因此，由式(13)即得式(21)。同样，由式(14)推出式(22)。

推论7的证明 由定义知$\sigma(1)=1$。下面来证式(8)。由式(20)及(21)推得

$$\begin{aligned}\sigma(a)&=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_s=0}^{\alpha_s}p_1^{e_1}\cdots p_s^{e_s}\\&=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_{s-1}=0}^{\alpha_{s-1}}p_1^{e_1}\cdots p_{s-1}^{e_{s-1}}\left(\sum_{e_s=0}^{\alpha_s}p_s^{e_s}\right)\\&=\left(\sum_{e_s=0}^{\alpha_s}p_s^{e_s}\right)\cdot\left(\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_{s-1}=0}^{\alpha_{s-1}}p_1^{e_1}\cdots p_{s-1}^{e_{s-1}}\right).\end{aligned}$$

继续对上式右边的累次求和用以上的推导，最后就得

$$\sigma(a)=\left(\sum_{e_1=0}^{\alpha_1}p_1^{e_1}\right)\cdots\left(\sum_{e_s=0}^{\alpha_s}p_s^{e_s}\right)=\sigma(p_1^{\alpha_1})\cdots\sigma(p_s^{\alpha_s}),$$

利用等比数列求和公式，由此即得式(8)。

例 1 证明：$(a,[b,c])=[(a,b),(a,c)]$。

证 若 $a=0$，等式显然成立。所以可设 a,b,c 是正整数，

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad b=p_1^{\beta_1}\cdots p_s^{\beta_s},\quad c=p_1^{\gamma_1}\cdots p_s^{\gamma_s}.$$

由推论 4 可得

$$(a,[b,c])=p_1^{\eta_1}\cdots p_s^{\eta_s},$$
$$\eta_j=\min(\alpha_j,\max(\beta_j,\gamma_j)),\quad 1\leqslant j\leqslant s.$$

$$[(a,b),(a,c)]=p_1^{\tau_1}\cdots p_s^{\tau_s},$$
$$\tau_j=\max(\min(\alpha_j,\beta_j),\min(\alpha_j,\gamma_j)),\quad 1\leqslant j\leqslant s.$$

容易验证，无论 $\alpha_j,\beta_j,\gamma_j$ 有怎样的大小关系，总有 $\tau_j=\eta_j(1\leqslant j\leqslant s)$成立，这就证明了所要的结论。这种关系式要直接用 § 4的方法来证是较困难的。

例 2 对 $a=180=2^2\cdot3^2\cdot5$，我们有

$$\tau(a)=(2+1)(2+1)(1+1)=18,$$

$$\sigma(a)=\frac{2^3-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1}$$

$$=7\cdot13\cdot6=546.$$

例 3 求 $\sum\limits_{d\mid a}\frac{1}{d}$。

解 由 § 2 定理 2 知

$$\sum_{d\mid a}\frac{1}{d}=\sum_{d\mid a}\frac{1}{(a/d)}=\frac{1}{a}\sum_{d\mid a}d=\frac{1}{a}\sigma(a).$$

由此及例 2 可得

$$\sum_{d\mid 180}\frac{1}{d}=\frac{1}{180}\sigma(180)=\frac{91}{30}.$$

习 题 六

1．证明：$g\mid A$的充要条件是对任意的 $p^\alpha\parallel g$(p 为素数)必有

$p^\alpha | A$，这里 $p^\alpha \| g$ 表示 $p^\alpha | g, p^{\alpha+1} \nmid g$。

2．设 $g|ab, g|cd$ 及 $g|ac+bd$。证明：$g|ac, g|bd$。

3．利用§6定理2及其推论来证明§4习题四(Ⅱ)的第8,9,10,11,12,14,15题。

4．设 a,b,n 是正整数 $a>b$。证明：若 $n|(a^n-b^n)$，则

$$n|(a^n-b^n)/(a-b)。$$

5．求满足 $\tau(n)=6$ 的最小正整数 n。

6．(i) 分别求出最小正整数 a，使得 $\sigma(n)=a$ 无解、恰有一个解、恰有两个解及恰有三个解。

(ii) 存在无穷多个 a 使 $\sigma(n)=a$ 无解。

7．证明：(i) $\tau(ab)\leqslant\tau(a)\tau(b)$；(ii) $\sigma(ab)\leqslant\sigma(a)\sigma(b)$，等号都当且仅当 $(a,b)=1$ 时成立(用两种不同的方法证明)。

8．证明：(i) $\tau(n)$ 是奇数的充要条件是 n 是完全平方数；

(ii) $\prod\limits_{d|n} d = n^{\tau(n)/2}$(用两种方法证明)。

9．$\sigma(n)$ 是奇数的充要条件是 $n=k^2$ 或 $2k^2$。

10．设 t 是实数，$\sigma_t(n)=\sum\limits_{d|n} d^t$。证明：$\sigma_t(n)=n^t\sigma_{-t}(n)$。并求 $\sigma_t(n)$ 的计算公式。

11．证明：任一正整数 n 必可唯一地表为 ab^2，其中 a,b 为正整数，且 a 不能为大于1的平方数整除(这种数称为无平方因子数)。

12．一个正整数 m 称为是完全数，如果 $\sigma(m)=2m$。试求出最小的两个完全数。

13．正整数 m 是完全数的充要条件是 $\sum\limits_{d|m} 1/d = 2$。

14．整数 n 是素数的充要条件是 $\sigma(n)=n+1$。

15．若 2^k-1 是素数，则 $2^{k-1}(2^k-1)$ 是完全数。

16．若 $\sigma(n)=n+k<2n$ 且 $k|n$，则 n 是素数。

17．若$2|m$，m是完全数，则$m=2^{k-1}(2^k-1)$，2^k-1是素数．

18．若奇数m是完全数，则必有$m=p^{4l+1}m_1^2$，其中p为$4k+1$形式的素数，$p\nmid m_1$．

19．设$\omega(n)$表n的不同的素因子个数（例如：$\omega(15)=2$，$\omega(8)=1$），d是无平方因子数．证明：满足$[d_1,d_2]=d$的正整数对d_1,d_2共有$3^{\omega(d)}$组（两组解d_1,d_2,d'_1,d'_2称为是不同的，只要$d_1\neq d'_1$或$d_2\neq d'_2$有一成立）．

20．设g,l是正整数，$g|l$．证明：满足$(x,y)=g,[x,y]=l$的正整数对x,y共有2^k组，这里$k=\omega(l/g)$（见上题）．

21．设n是奇数．求n表为两整数平方之差的表法有多少种？

22．证明：$\log_2 10,\log_3 7,\log_{15}21$都是无理数．

§7* 算术基本定理(B)

本节将不利用§4中关于最大公约数的结论，直接证明算术基本定理（§6定理2）和§6定理1，并证明这两个定理是等价的．

算术基本定理（§6定理2）的直接证明 用反证法．假设结论不成立．设$a_0>1$是使结论不成立的最小正整数．由§2定理5知，a_0必可表为素数之积，因此，它必有两种不同的素数分解式，设为

$$a_0=p_1\cdots p_s=q_1\cdots q_r,$$

其中p_j,q_i都是素数．不妨设$p_1\leqslant\cdots\leqslant p_s$，$q_1\leqslant\cdots\leqslant q_r$．由素数定义知，$a_0$一定不是素数，所以必有

$$s\geqslant 2,\quad r\geqslant 2. \tag{1}$$

其次，由a_0的最小性知，对任意的j和i必有

$$p_j\neq q_i. \tag{2}$$

不妨设$q_1>p_1$．这样，有

$$1<b_0=a_0-p_1q_2\cdots q_r=(q_1-p_1)q_2\cdots q_r<a_0. \tag{3}$$

显然有$p_1|b_0$，即$b_0=p_1b_1$，由此及§2定理3得到b_0的素数分解式：

$$b_0 = p_1 p'_2 \cdots p'_u, \tag{4}$$

其中$p'_2,\cdots,p'_u$是素数，$b_1 = p'_2 \cdots p'_u$(当$b_1 = 1$时，它们不出现)。但另一方面，当$q_1 - p_1 = 1$时，得到b_0的素数分解式

$$b_0 = q_2 \cdots q_r; \tag{5}$$

当$q_1 - p_1 > 1$时，由§2定理5知必有$q_1 - p_1$的素数分解式：

$$q_1 - p_1 = q_{11} \cdots q_{1v},$$

$q_{1j}(1 \leqslant j \leqslant v)$是素数。因而得到$b_0$的素数分解式：

$$b_0 = q_{11} \cdots q_{1v} q_2 \cdots q_r. \tag{6}$$

由素数的定义、q_1和p_1都是素数及$q_1 \neq p_1$知，$p_1 \nmid q_1 - p_1$。由此及式(2)知，在b_0的素数分解式(5)或(6)中一定不会出现p_1，所以(5)或(6)一定是和(4)不同的素数分解式。但由式(3)知，这和a_0的最小性矛盾。证毕。

下面来给出§6定理1的两个直接证明。

§6定理1的直接证明(一) 只要证$k = 2$的情形，且可假定$a_1 \geqslant 1, a_2 \geqslant 1$。用反证法。假设结论不成立。由最小自然数原理知，必有最小的素数p_0使结论不成立，即存在a_1, a_2使

$$p_0 | a_1 a_2, \quad p_0 \nmid a_1, \quad p_0 \nmid a_2. \tag{7}$$

考虑由所有这样的数对$\{a_1, a_2\}$组成的集合T。由最小自然数原理知，必有a_1^*, a_2^*属于这集合，而使乘积$a_1^* a_2^*$最小。这时必有

$$1 < a_1^* < p_0, \quad 1 < a_2^* < p_0. \tag{8}$$

因若不然，比如说有$a_1^* > p_0$，则由带余数除法可得

$$a_1^* = q p_0 + r_1, \quad 0 < r_1 < p_0.$$

这样，数对$\{r_1, a_2^*\}$也满足条件(7)。但$r_1 a_2^* < a_1^* a_2^*$，和$a_1^* a_2^*$的最小性矛盾。设

$$a_1^* a_2^* = p_0 c.$$

由式(8)及p_0是素数知$2 \leqslant c < p_0$。进而由§2定理4知，必有素数$p_1 | c$。由$p_1 < p_0$及p_0的最小性知，$p_1 | a_1^*$和$p_1 | a_2^*$至少有一个成立。设$p_1 | a_1^*$，则有

$$\left(\frac{a_1^*}{p_1}\right) a_2^* = p_0 \left(\frac{c}{p_1}\right).$$

显见，数对$\{a_1^*/p_1, a_2^*\}$也属于集合T，但这和$a_1^*a_2^*$的最小性矛盾。证毕。

§6定理1的直接证明(二) 不妨设$a_1>0$，$a_2>0$。若$p\nmid a_1$，考虑数列$a_1, 2a_1, 3a_1, \cdots, ka_1, \cdots$。这数列中必有数可被$p$整除，例如$pa_1$即是。由最小自然数原理知这数列中必有一最小正整数被p整除，设为na_1。显见$1<n\leqslant p$。我们来证明$n=p$。若不然，由带余数除法知

$$p=qn+r,\quad 1\leqslant r<n,$$

这里$r\geqslant 1$是因为p是素数，$n\nmid p$。由此推出$p|ra_1$，这和na_1的最小性矛盾。最后来证明$p|a_2$。由带余数除法知

$$a_2=qp+r,\quad 0\leqslant r<p.$$

所以$p|ra_1$。由此及pa_1的最小性推出$r=0$，即$p|a_2$。证毕。

下面来证明

定理1 §6定理1和§6定理2等价。

证 §6定理1成立$\Longrightarrow$§6定理2成立 这就是§6中给出的§6定理2的证明(注意：在这证明中除了§6定理1的结论，及整除的定义、素数的定义和§2定理5外，没用其它任何知识)。

§6定理2成立$\Longrightarrow$§6定理1成立 只要证$k=2$的情形。用反证法，设有素数p_0，正整数a_1, a_2满足

$$p_0|a_1a_2,\quad p_0\nmid a_1,\quad p_0\nmid a_2.$$

显见，必有$a_1\geqslant 2$，$a_2\geqslant 2$，$a_1a_2/p\geqslant 2$。由§2定理5知有素数分解式：

$$a_1=p_{11}\cdots p_{1r},$$

$$a_2=p_{21}\cdots p_{2s},$$

$$(a_1a_2)/p_0=p_1\cdots p_t.$$

由$p_0\nmid a_1$知$p_{1j}\neq p_0(1\leqslant j\leqslant r)$；由$p_0\nmid a_2$知$p_{2j}\neq p_0(1\leqslant j\leqslant s)$。这样，由以上三式就得到了$a_1a_2$的两种不同的素数分解式：

$$a_1a_2=p_{11}\cdots p_{1r}p_{21}\cdots p_{2s},$$

$$a_1a_2=p_0p_1\cdots p_t.$$

这和§6定理2成立矛盾。证毕(注意：在这证明中除了§6定理2的结论，及整除、素数的定义和§2定理5之外没有用其它知识)。

§6的定理1是证明了正整数中的素数的一个性质，§6定理2是证明了正整数表为素数的乘积的表法是唯一的(不计次序)。这两个看来极为“明显”的结论，为什么还要证明呢？而且给出了不同的证明，还作了深入的讨论。这究竟有没有必要呢？有兴趣的读者可参看附录二。

最后，我们要指出的是：由于我们直接证明了算术基本定理，进而也就得到§6的推论3、推论4——关于除数、最大公约数、最小公倍数的表示式，而在所有的论证中，除了§4定理1之外，§4的所有其它结论都用不到。相反的可以用推论3、推论4来证明§4定理2—定理12，而且论证更为直观易懂。这些请读者自己讨论。此外，虽然我们证明了每个合数都可唯一分解为素数的乘积，但如何实现这种分解，特别是大数的分解，至今还没有有效方法。

习 题 七

1．证明：在整数集合 $\boldsymbol{Z}$ 中关于两个整数 $u_0,u_1(u_1\neq 0)$ 的最大公约数 (u_0,u_1) 的以下五种定义是等价的。

(i) (u_0,u_1) 是 u_0,u_1 的公约数中的最大的。

(ii) (u_0,u_1) 是 u_0,u_1 的这样一个公约数 D：$D>0$，及对 u_0,u_1 的任一公约数 d 必有 $d\mid D$。

(iii) (u_0,u_1) 是形如 u_0x+u_1y 的正整数中的最小的。

(iv) (u_0,u_1) 是§5定理1中的 u_{k+1}。

(v) 若 u_0,u_1 的素因数分解式是

$$u_0=p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad u_1=p_1^{\beta_1}\cdots p_s^{\beta_s},$$

定义 $(u_0,u_1)=p_1^{\delta_1}\cdots p_s^{\delta_s}$，其中 $\delta_j=\min(\alpha_j,\beta_j)$，$1\leqslant j\leqslant s$。详细

论述这五种定义的合理性与特点，以及如何从每一种定义出发来建立整除理论。

2．找几本不同的初等数论教科书，分析它们是如何建立整除理论的。

§8 符号[x]，n!的分解式

定义1 设 x 是实数，$[x]$表示不超过 x 的最大整数，称为 x 的**整数部分**，即$[x]$是一个整数且满足

$$[x]\leqslant x<[x]+1. \tag{1}$$

例如：$[1.2]=1$，$[-1.2]=-2$，$[3]=3$，$[-4]=-4$。

记$\{x\}=x-[x]$，称为 x 的**小数部分**。由(1)知

$$0\leqslant\{x\}<1. \tag{2}$$

x 是整数的充要条件是$\{x\}=0$。例如

$$\{1.2\}=0.2,\ \{-1.2\}=0.8,\ \{3\}=\{-4\}=0.$$

$[x]$和$\{x\}$是数学中十分有用的两个符号。下面来列出它们的性质，证明很简单，关键是要学会灵活运用这些性质。

定理1 设x,y是实数。我们有

(i) 若$x\leqslant y$，则$[x]\leqslant[y]$。

(ii) 若$x=m+v$，m是整数，$0\leqslant v<1$，则$m=[x]$，$v=\{x\}$。特别地，当$0\leqslant x<1$时，$[x]=0$，$\{x\}=x$。

(iii) 对任意整数m有：$[x+m]=[x]+m$，$\{x+m\}=\{x\}$。$\{x\}$是周期为1的周期函数。$[x]$和$\{x\}$的图形分别见图1和图2。

(iv) $[x]+[y]\leqslant[x+y]\leqslant[x]+[y]+1$，其中等号有且仅有一个成立。

(v)

$$[-x]=\begin{cases}-[x], & x\in\boldsymbol{Z},\\ -[x]-1, & x\notin\boldsymbol{Z}\end{cases}$$

及

$$\{-x\}=\begin{cases}-\{x\}=0, & x\in \boldsymbol{Z},\\ 1-\{x\}, & x\notin \boldsymbol{Z}.\end{cases}$$

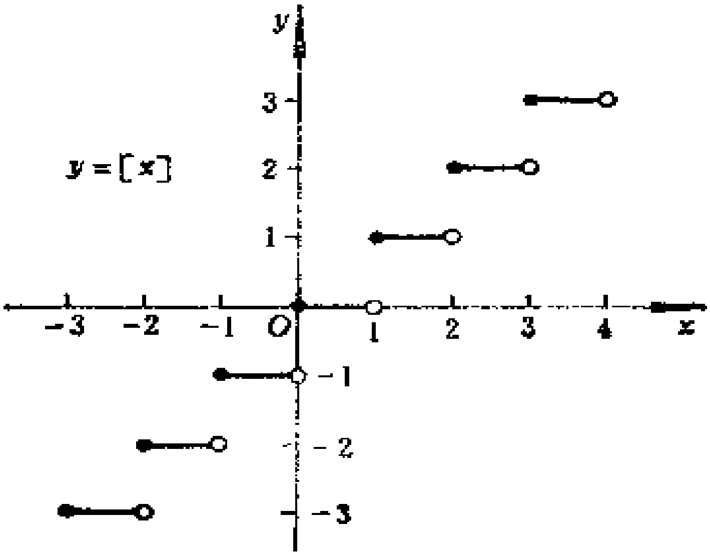


图 1

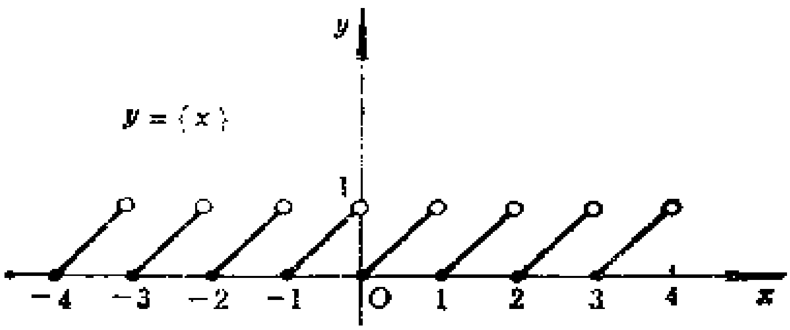


图 2

(vi) 对正整数 m 有 $\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right]$。

(vii) 不小于 x 的最小整数是 $-[-x]$。

(viii) 小于 x 的最大整数是 $-[-x]-1$。

(ix) 大于 x 的最小整数是 $[x]+1$。

(x) 离 x 最近的整数是 $[x+1/2]$ 和 $1-[-x+1/2]$。当 $x+1/2$ 是整数时，这两个不同的整数和 x 等距；当 $x+1/2$ 不是整数时，

它们相等。

(xi) 若$x\geqslant 0$，则不超过x的正整数n的个数等于$[x]$，即

$$\sum_{1\leqslant n\leqslant x} 1=[x].$$

(xii) 设a和N是正整数。那么，正整数$1,2,\cdots,N$中被a整除的正整数的个数是$[N/a]$。

证 (i) 由$[x]\leqslant x\leqslant y<[y]+1$即得。

(ii) 由$m\leqslant x<m+1$推出。

(iii) 由$[x]+m\leqslant x+m<([x]+m)+1$推出。

(iv) $x+y=[x]+[y]+\{x\}+\{y\}$，及$0\leqslant\{x\}+\{y\}<2$。当$0\leqslant\{x\}+\{y\}<1$时，由(ii)知$[x+y]=[x]+[y]$；当$1\leqslant\{x\}+\{y\}<2$时，$x+y=[x]+[y]+1+(\{x\}+\{y\}-1)$，由(ii)知$[x+y]=[x]+[y]+1$。

(v) x为整数时显然成立。x不是整数时，$-x=-[x]-\{x\}=-[x]-1+1-\{x\}$，$0<1-\{x\}<1$，由(ii)知成立。

(vi) 由带余数除法知，存在整数q,r使得

$$[x]=qm+r,\quad 0\leqslant r<m,$$

即

$$[x]/m=q+r/m,\quad 0\leqslant r/m<1.$$

由此及(ii)推出$[[x]/m]=q$。另一方面

$$x/m=[x]/m+\{x\}/m=q+(\{x\}+r)/m.$$

注意到$0\leqslant(\{x\}+r)/m<1$，由此及(ii)推出$[x/m]=q$。所以(v)成立。

(vii) 设不小于x的最小整数是a，即$a-1<x\leqslant a$。因此，$-a\leqslant -x<-a+1$，所以$-a=[-x]$，即$a=-[-x]$。

(viii)和(ix)的证明留给读者，方法与(vii)相同。

(x) 离x最近的整数必在$[x]$和$[x]+1$之中。当$x+1/2$是整数时，这两数和x等距。容易验证$[x]+1=[x+1/2]$，及$[x]=-[-x+1/2]$。当$x+1/2$不是整数时，若$\{x\}<1/2$，则离x最近

的整数是$[x]$。因$x+1/2=[x]+\{x\}+1/2$，$0\leqslant\{x\}+1/2<1$，由(ii)知$[x]=[x+1/2]$；若$1/2<\{x\}<1$，则离x最近整数是$[x]+1$。因$x+1/2=[x]+1+\{x\}-1/2$，$0<\{x\}-1/2<1$，由(ii)知$[x]+1=[x+1/2]$。在$x+1/2$不是整数时，由(v)知

$$\begin{aligned}[x+1/2]&=-[-x-1/2]-1\\&=-[-x+1/2-1]-1=-[-x+1/2],\end{aligned}$$

最后一步用到了(iii)。证毕。

(xi) 由于整数$n\leqslant x$就是$n\leqslant[x]$，所以成立。

(xii) 被a整除的正整数是$a,2a,3a,\cdots$。设$1,2,\cdots,N$中被a整除的正整数个数为k，那么必有$ka\leqslant N<(k+1)a$，即$k\leqslant N/a<k+1$，所以成立。

例 1 平面上坐标为整数的点称为整点或格点。设$x_1<x_2$是实数，$y=f(x)$ $(x_1<x\leqslant x_2)$是非负连续函数。证明：

(i) 区域：$x_1<x\leqslant x_2$，$0<y\leqslant f(x)$上的整点的个数

$$M=\sum_{x_1<n\leqslant x_2}[f(n)],$$

这里变数n取整数值；

(ii)

$$[x_1]-[x_2]<M-\sum_{x_1<n\leqslant x_2}f(n)\leqslant 0.$$

证 先来证明(i)。所说区域上的整点，都在这样的直线段上：$x=n$，$1\leqslant y\leqslant f(n)$，$n$是一满足$x_1<n\leqslant x_2$的整数。而直线段$x=n$，$1\leqslant y\leqslant f(n)$上的整点数就是满足$1\leqslant y\leqslant f(n)$的整数$y$的个数，由定理1(xi)知等于$[f(n)]$(见图3)。这就证明了(i)。由小数部分的定义知

$$\sum_{x_1<n\leqslant x_2}[f(n)]=\sum_{x_1<n\leqslant x_2}f(n)-\sum_{x_1<n\leqslant x_2}\{f(n)\},$$

所以

$$M-\sum_{x_1<n\leqslant x_2} f(n)=-\sum_{x_1<n\leqslant x_2}\{f(n)\}. \tag{3}$$

由式(2)知

$$0\leqslant \sum_{x_1<n\leqslant x_2}\{f(n)\}<\sum_{x_1<n\leqslant x_2}1.$$

由整数部分的定义及定理 1 (ix)知

$$\sum_{x_1<n\leqslant x_2}1=\sum_{[x_1]+1\leqslant n\leqslant [x_2]}1=[x_2]-[x_1].$$

由以上三式就证明了(ii)。当 $f(x)$ 取不同的函数时，会由此得一些有趣的结果，这将放在习题中。

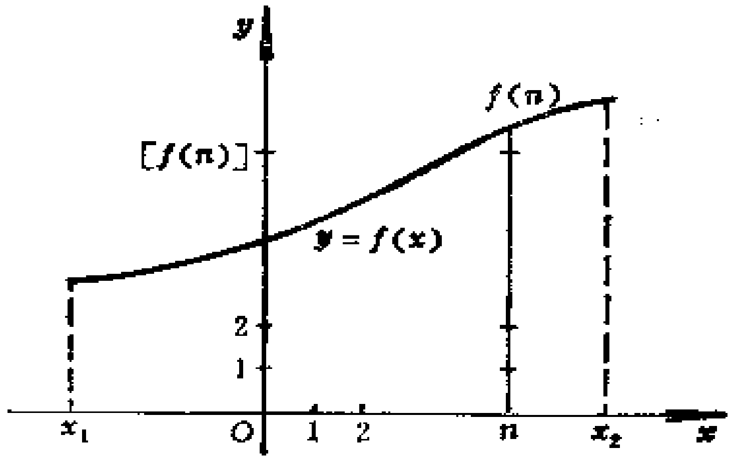


图 8

下面来求 $n!$ 的标准素因数分解式。若素数 $p|n!$，则由§6定理 1 知必有 $p|k$，k 为某个正整数 $\leqslant n$；另一方面，任一素数 $p\leqslant n$ 必有 $p|n!$。所以，由§6 定理 2 知 $n!$ 的标准素因数分解式必为

$$n!=p_1^{\alpha_1}\cdots p_s^{\alpha_s}, \tag{4}$$

这里 $2=p_1<p_2<\cdots<p_s\leqslant n$ 是所有不超过 n 的素数。这样，为了求出分解式(4)，只需要去确定方次数 α_j $(1\leqslant j\leqslant s)$。

先引进一个符号。设 k 是非负整数，记号

$$a^k \| b \tag{5}$$

表示 b 恰被 a 的 k 次方整除，即

$$a^k | b, \quad a^{k+1} \nmid b. \tag{6}$$

定理2 设 n 是正整数，p 是素数。再设 $\alpha = \alpha(p,n)$ 满足 $p^\alpha \| n!$。那么

$$\alpha = \alpha(p,n) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right]. \tag{7}$$

证 式(7)右边实际上是一有限和，因为必有整数 k 满足 $p^k \leqslant n < p^{k+1}$，这样，式(7)就是

$$\alpha = \sum_{j=1}^{k} \left[\frac{n}{p^j}\right]. \tag{8}$$

设 j 是给定的正整数，c_j 表示$1,2,\cdots,n$ 中能被 p^j 整除的数的个数，d_j 表示 $1,2,\cdots,n$ 中恰被 p 的 j 次方整除的数的个数。显见，

$$d_j = c_j - c_{j+1}.$$

由定理 1 (xii)知

$$c_j = [n/p^j],$$

因而，

$$d_j = [n/p^j] - [n/p^{j+1}]. \tag{9}$$

容易看出，当 $j > k$ 时 $d_j = 0$，以及

$$\alpha = 1 \cdot d_1 + 2 \cdot d_2 + \cdots + k \cdot d_k. \tag{10}$$

后者是因为我们可把 $1,2,\cdots,n$ 分为这样两两不交的 k 个集合：第 j 个集合由 $1,2,\cdots,n$ 中恰被 p^j 整除的数组成。这样，第 j 个集合的所有数的乘积恰被 p 的 $j \cdot d_j$ 次方整除，由此即得式(10)。进而，由式(9)及(10)就推出式(8)(注意：$[n/p^{k+1}] = 0$)。证毕。

推论 3 设 n 是正整数。我们有

$$n! = \prod_{p \le n} p^{\alpha(p,n)}, \tag{11}$$

这里连乘号表示对所有不超过 n 的素数求积，$\alpha(p,n)$ 由式(7)给

出。

推论 3 可以由定理 2 及一开头的讨论立即推出。此外显然有

$$\alpha(p_1,n)\leqslant\alpha(p_2,n),\quad p_2<p_1. \tag{12}$$

例 2 求20!的标准素因数分解式.

不超过20的素数有2,3,5,7,11,13,17,19.由定理 2 知:

$$\alpha(2,20)=\left[\frac{20}{2}\right]+\left[\frac{20}{4}\right]+\left[\frac{20}{8}\right]+\left[\frac{20}{16}\right]$$

$$=10+5+2+1=18.$$

$$\alpha(3,20)=\left[\frac{20}{3}\right]+\left[\frac{20}{9}\right]=6+2=8.$$

$$\alpha(5,20)=\left[\frac{20}{5}\right]=4.\quad \alpha(7,20)=\left[\frac{20}{7}\right]=2.$$

$$\alpha(11,20)=\left[\frac{20}{11}\right]=1.\quad \alpha(13,20)=\left[\frac{20}{13}\right]=1.$$

$$\alpha(17,20)=\left[\frac{20}{17}\right]=1.\quad \alpha(19,20)=\left[\frac{20}{19}\right]=1.$$

所以,

$$20!=2^{18}\cdot 3^8\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19.$$

例 3 20!的十进位表示中有多少个零?

这就是要求正整数 k,使 $10^k\|20!$。由上例知 $k=4$,即是 5 的方次数。所以结尾有四个零。

例 4 设整数 $a_j>0$ $(1\leqslant j\leqslant s)$,$n=a_1+a_2+\cdots+a_s$。证明:$n!/(a_1!a_2!\cdots a_s!)$是整数。

证 用定理 2 的符号,只要证明对任意素数 p 必有

$$\alpha(p,n)\geqslant\alpha(p,a_1)+\alpha(p,a_2)+\cdots+\alpha(p,a_s).$$

而由式(7)知这可以从下面不等式推出:对任意 $j\geqslant 1$ 有

$$\left[\frac{n}{p^j}\right]\geqslant\left[\frac{a_1}{p^j}\right]+\left[\frac{a_2}{p^j}\right]+\cdots+\left[\frac{a_s}{p^j}\right].$$

由 $n=a_1+\cdots+a_s$ 及定理 1 (iv)知上述不等式成立。证毕。

熟知，可用排列组合方法来证明 $n!/(a_1!\cdots a_s!)$是整数，它称为是多重组合数，这里用数论方法给了一个新证明。特别当 $s=2$时，证明了

$$\binom{n}{a_1}=\frac{n!}{a_1!(n-a_1)!}=\frac{n(n-1)\cdots(n-a_1+1)}{a_1!} \tag{13}$$

是整数，这就是说，a_1 个相邻正整数的乘积可被 $a_1!$ 整除。由此立即得到

推论4 m 个相邻整数的乘积可被 $m!$整除。

应该指出，例 4 是一个简单情形。在习题八第29题中，要证明 $n!(m!)^n\mid(mn)!$。这等价于要证明对任意的素数 p 有

$$\alpha(p,mn)\geqslant\alpha(p,n)+n\cdot\alpha(p,m). \tag{14}$$

但这里 $mn<n+m+\cdots+m$(有 n 个 m)，我们不能证明对每个 $j\geqslant 1$ 必有

$$\left[\frac{mn}{p^j}\right]\geqslant\left[\frac{n}{p^j}\right]+n\left[\frac{m}{p^j}\right],$$

因而不能用例 4 的简单办法来证，而要直接证明式(14)成立。具体论证见解答。当然，这结论可用排列组合法来证，而且比较简单(留给读者)。

习 题 八

1．设 a,b 是整数，$a\geqslant1$，$b=qa+r$，$0\leqslant r<a$。证明：

$$q=[b/a],\quad r=a\{b/a\}.$$

2．设 a,b 是整数，$a\geqslant1$，$b=q_1a+r_1$，$-a/2\leqslant r_1<a/2$。证明：

$$q_1=\left[\frac{2b}{a}\right]-\left[\frac{b}{a}\right],\quad r_1=a\left\{\frac{2b}{a}\right\}-a\left\{\frac{b}{a}\right\}.$$

3. 证明：对任意正实数 x,y 有$[xy]\geqslant[x][y]$. 试讨论$\{xy\}$和$\{x\}\{y\}$之间会有怎样的关系。

4. 证明：对任意实数 x 有$[x]+[x+1/2]=[2x]$。

5. 证明：对任意整数 $n\geqslant 2$ 及实数 x 有

$$[x]+[x+1/n]+\cdots+[x+(n-1)/n]=[nx].$$

6. 设 m,n 是整数，$n\geqslant 1$。证明：

$$\left[\frac{m+1}{n}\right]=\begin{cases}\left[\dfrac{m}{n}\right], & \text{当 } n\nmid m+1,\\ \left[\dfrac{m}{n}\right]+1, & \text{当 } n\mid m+1.\end{cases}$$

7. 若$[x+y]=[x]+[y]$, $[-x-y]=[-x]+[-y]$同时成立，则 x,y 必有一个是整数。

8. 证明：对任意实数 x,y 有

$$[x-y]\leqslant[x]-[y]\leqslant[x-y]+1.$$

9. 证明：(i) 对任意实数 α,β 有$[2\alpha]+[2\beta]\geqslant[\alpha]+[\beta]+[\alpha+\beta]$。但不一定有$[3\alpha]+[3\beta]\geqslant[\alpha]+[\beta]+[2\alpha+2\beta]$成立；

(ii) 设 m,n 是正整数。对任意实数 α,β 有

$$[(m+n)\alpha]+[(m+n)\beta]\geqslant[m\alpha]+[m\beta]+[n\alpha+n\beta]$$

成立的充要条件是 $m=n$。

10. 试决定对怎样的实数 x 有下面的等式成立：

(i) $[x+3]=3+x$；　　(ii) $[x]+[x]=[2x]$；

(iii) $[11x]=11$；　　(iv) $[11x]=10$；

(v) $[x+1/2]+[x-1/2]=[2x]$。

11. 证明：对任意实数 x,y 有$\{x+y\}\leqslant\{x\}+\{y\}$。

12. 设$\|x\|$表示实数 x 离最近整数的距离。证明：

(i) $\|x\|=\min(\{x\},1-\{x\})$；

(ii) 对任意整数 n 有$\|x+n\|=\|x\|$；

(iii) $\|x\|=\|-x\|$；

(iv) $\|x+y\|\leqslant\|x\|+\|y\|$；

(v) $\|x-y\|\geqslant\|x\|-\|y\|$；

(vi) 画出 $y=\|x\|$ 的图形。

13. 设 m 是正整数。证明：

(i) $2^{m+1}\|[(1+\sqrt{3})^{2m+1}]$；

(ii) $[\sqrt{m}+\sqrt{m+1}]=[\sqrt{m}+\sqrt{m+2}]$。

14. 设 $0<\theta\leqslant 1$ 是实数，n 是正整数。再设

$$a_n=\begin{cases}0, & 当[n\theta]=[(n-1)\theta],\\ 1, & 其它情形.\end{cases}$$

证明：$a_1+\cdots+a_n=[n\theta]$。

15. 设 m,n 是正整数，$(m,n)=1$. 证明：

(i) 在以坐标为 $\{0,0\}$, $\{0,m\}$, $\{n,0\}$, $\{n,m\}$ 为顶点的矩形内部有 $(m-1)(n-1)$ 个整点；

(ii) $\sum\limits_{s=1}^{n-1}\left[\dfrac{ms}{n}\right]=\dfrac{1}{2}(m-1)(n-1)$.

16. 设 m,n 是奇正整数，$(m,n)=1$。证明

$$\sum_{0<s<m/2}\left[\frac{n}{m}s\right]+\sum_{0<t<n/2}\left[\frac{m}{n}t\right]=\frac{m-1}{2}\cdot\frac{n-1}{2}.$$

17. 设实数 $C>0$。M 是区域：$x>0$，$y>0$，$xy\leqslant C$ 上的整点。证明：

(i) $M=\sum\limits_{1\leqslant s\leqslant C}\left[\dfrac{C}{s}\right]$；

(ii) $M=2\sum\limits_{1\leqslant s\leqslant\sqrt{C}}\left[\dfrac{C}{s}\right]-[\sqrt{C}]^2$；

(iii) $M=\sum\limits_{1\leqslant s\leqslant C}\tau(s)$.

(iv) 分别利用(i),(ii)给出计算 M 的近似公式。

18. 设实数 $R>0$，M 是区域 $x^2+y^2\leqslant R^2$ 上的整点数。证

明：

(i) $M = 1 + 4[R] + 4\sum_{1\leqslant s\leqslant R}[\sqrt{R^2 - s^2}]$；

(ii) $M = 1 + 4[R] + 8\sum_{1\leqslant s\leqslant R/\sqrt{2}}[\sqrt{R^2 - s^2}] - 4[R/\sqrt{2}]^2$。

19．求 2,3,6,12 及 70 整除 623!的最高方幂．

20．求120!的十进制表达式中结尾有多少个零。

21．§8的式(7)当 p 是合数时成立吗？举例说明。

22．求32!的素因数分解式．

23．设 p 是素数，n 是正整数。

(i) 求 $p^e \| (2n)!!$中的 e 的计算公式，这里

$$(2n)!! = (2n)(2n-2)\cdots 2;$$

(ii) 求 $p^f \| (2n-1)!!$中的 f 的计算公式，这里

$$(2n-1)!! = (2n-1)(2n-3)\cdots 1。$$

24．用例 4 的方法证明 $n!(n-1)! \mid (2n-2)!$．

25．设 a,b 是正整数，$(a,b)=1$。再设 ρ 是一实数。证明：若 $a\rho, b\rho$ 是整数，则 ρ 也是整数。

26．设 a,b 是正整数，$(a,b)=1$。证明：$a!b! \mid (a+b-1)!$。

27．设 $\alpha(p,n)$由§8定理 2 给出，证明：$\alpha(p,n) < n/(p-1)$。

28．证明：$(2n)!/(n!)^2$ 是偶数。

29．设 m,n 是正整数。证明：$n!(m!)^n \mid (mn)!$．

30．设 a,b 是正整数。证明：$a!b!(a+b)! \mid (2a)!(2b)!$．

31．求组合数$\binom{n}{1},\binom{n}{2},\cdots,\binom{n}{n-1}$的最大公约数。

32．设 p 是一个给定的素数．证明：一定存在正整数 a，使对任意的正整数 n，不可能有 $p^a \| n!$。试提出一个决定所有这种 a 的方法。

33．设正整数 n 的 p 进位表示是：

$$n = a_0 + a_1 p + \cdots + a_k p^k,$$

$$0\leqslant a_j<p,\quad 0\leqslant j\leqslant k-1,\quad 1\leqslant a_k<p.$$

证明：(i) $a_j=[n/p^j]-[n/p^{j+1}]$，$0\leqslant j\leqslant k$；(ii) 若 p 是素数，$\alpha(p,n)$由§8定理2给出，则

$$\alpha(p,n)=\frac{n-A_n}{p-1},\quad A_n=a_0+a_1+\cdots+a_k.$$

34. 设 n,a,b 是正整数。证明：

$$n!\mid b^{n-1}a(a+b)\cdots(a+(n-1)b).$$

35. 设 α 是正实数。再设 $a_n=[n(1+\alpha)]$，$n=1,2,\cdots$；$b_n=[n(1+\alpha^{-1})]$，$n=1,2,\cdots$。证明：这些数两两不相等，且恰好给出了全体正整数的充要条件是 α 是正无理数。

36. 设 α,β 是正实数。再设 $a_n=[n\alpha]$，$n=1,2,\cdots$；$b_n=[n\beta]$，$n=1,2,\cdots$。证明：这些数两两不相等，且恰好给出了全体正整数的充要条件是：α,β 为正无理数且满足

$$\frac{1}{\alpha}+\frac{1}{\beta}=1.$$

第二章 不定方程(I)

变数为整数的方程称为不定方程。不定方程是数论中的一个十分重要的课题。本章讨论能直接利用整除理论来判断其是否有解，以及有解时求出其全部解的最简单的不定方程，即§1中的一次不定方程，§2中的不定方程 $x^2+y^2=z^2$——这个不定方程与边长为整数的直角三角形的性质有密切关系。在§2中利用研究 $x^2+y^2=z^2$ 的方法还讨论了几个与此相关的简单不定方程。

§1 一次不定方程

设整数 $k\geqslant 2$，$c,a_1,\cdots,a_k$ 是整数且 $a_1,\cdots,a_k$ 都不等于零，以及 $x_1,\cdots,x_k$ 是整数变数。方程

$$a_1x_1+\cdots+a_kx_k=c \tag{1}$$

称为 k 元一次不定方程，$a_1,\cdots,a_k$ 称为它的系数。

定理1 不定方程(1)有解的充要条件是 $(a_1,\cdots,a_k)\mid c$。进而，不定方程(1)有解时，它的解和不定方程

$$\frac{a_1}{g}x_1+\cdots+\frac{a_k}{g}x_k=\frac{c}{g} \tag{2}$$

的解相同，这里 $g=(a_1,\cdots,a_k)$。

证 必要性显然。若 $g\mid c$，设 $c=gc_1$。由第一章§4定理13知，必有整数 $y_{1,0},\cdots,y_{k,0}$ 使得

$$a_1y_{1,0}+\cdots+a_ky_{k,0}=g. \tag{3}$$

因此 $x_1=c_1y_{1,0},\cdots,\ x_k=c_1y_{k,0}$ 即为(1)的一组解，这就证明了充分性。由于(1)有解时必有 $g\mid c$，而这时不定方程(1)和(2)是同一个方程，这就证明了后一结论。

定理2 设二元一次不定方程

$$a_1x_1+a_2x_2=c \tag{4}$$

有解，$x_{1,0}$,$x_{2,0}$是它的一组解。那么，它的所有解为

$$\begin{cases} x_1=x_{1,0}+\dfrac{a_2}{(a_1,a_2)}t, \\ x_2=x_{2,0}-\dfrac{a_1}{(a_1,a_2)}t, \end{cases} \quad t=0,\pm1,\pm2,\cdots. \tag{5}$$

证　容易直接验证由式(5)给出的x_1,x_2，对所有整数t都满足不定方程(4)。反过来，设x_1,x_2是(4)的一组解，我们有

$$a_1x_1+a_2x_2=c=a_1x_{1,0}+a_2x_{2,0}.$$

进而有

$$a_1(x_1-x_{1,0})=-a_2(x_2-x_{2,0}),$$

$$\frac{a_1}{(a_1,a_2)}(x_1-x_{1,0})=-\frac{a_2}{(a_1,a_2)}(x_2-x_{2,0}).$$

因$\left(\dfrac{a_1}{(a_1,a_2)},\dfrac{a_2}{(a_1,a_2)}\right)=1$，由第一章§4定理11知$x_1-x_{1,0}=\dfrac{a_2t}{(a_1,a_2)}$.

进而由以上两式得$x_2-x_{2,0}=-\dfrac{a_1}{(a_1,a_2)}t$.这就证明了$x_1$,$x_2$可表为

式(5)的形式。证毕。

例1　求$10x_1-7x_2=17$的全部解。

解　容易看出，$(10,7)=1$，所以方程有解。由视察法可得$x_{1,0}=1$，$x_{2,0}=-1$是一组特解。因此全部解是

$$x_1=1-7t,\quad x_2=-1-10t,\quad t=0,\pm1,\pm2,\cdots.$$

例2　求$18x_1+24x_2=9$的解。

解　由$(18,24)=6\nmid 9$知无解。

求解不定方程(4)，必需(i)求出最大公约数$g=(a_1,a_2)$，并判断是否有$g|c$；(ii)若$g|c$，即有解，则设法去求出一组特解$x_{1,0}$,$x_{2,0}$.下面我们通过具体例子来介绍一种判定方程是否有解、及求出其解的直接算法。这种算法对$k>2$的情形也适用。

例 3 求 $907x_1+731x_2=2107$ 的解。

解

$$x_2=\frac{1}{731}(-907x_1+2107)$$
$$=-x_1+3+\frac{1}{731}\cdot(-176x_1-86)$$
$$x_3=\frac{1}{731}(-176x_1-86)\in \boldsymbol{Z}\text{①}$$

$$x_1=\frac{1}{176}(-731x_3-86)$$
$$=-4x_3+\frac{1}{176}(-27x_3-86)$$
$$x_4=\frac{1}{176}(-27x_3-86)\in \boldsymbol{Z}$$

$$x_3=\frac{1}{27}(-176x_4-86)$$
$$=-7x_4-3+\frac{1}{27}(13x_4-5)$$
$$x_5=\frac{1}{27}(13x_4-5)\in \boldsymbol{Z}$$

$$x_4=(27x_5+5)/13$$
$$=2x_5+(x_5+5)/13$$
$$x_6=(x_5+5)/13\in \boldsymbol{Z}$$
$$x_5=13x_6-5=-5+13x_6$$

$$x_4=2x_5+x_6$$
$$=2(-5+13x_6)+x_6$$
$$=-10+27x_6$$

$$x_3=-7x_4-3+x_5$$
$$=-7(-10+27x_6)-3+(-5+13x_6)$$
$$=62-176x_6$$

$$x_1=-4x_3+x_4$$
$$=-4(62-176x_6)+(-10+27x_6)$$
$$=-258+731x_6$$

$$x_2=-x_1+3+x_3$$
$$=-(-258+731x_6)+3+(62-176x_6)$$
$$=323-907x_6$$

这样就求出了全部解：

---

① 这是一个新的不定方程：$176x_1+731x_3=-86$。把原来关于 x_1，x_2 的不定方程转化为关于 x_1，x_3 的不定方程，且其系数绝对值比原方程小。下面就是反复这样做。

$$x_1 = -258 + 731x_6,\quad x_2 = 323 - 907x_6,\quad x_6 = 0, \pm 1, \pm 2, \cdots.$$

细心的读者不难发现，这种解不定方程的算法实际上是对整个不定方程用辗转相除法（见第一章§5），依次化为等价的不定方程，直至得到有一个变元的系数为±1的不定方程为止（在上例中是 $x_5 - 13x_6 = -5$），这样的不定方程是可以直接解出的（这里是 $x_5 = -5 + 13x_6$，$x_6 = 0, \pm 1, \pm 2, \cdots$）。再依次反推上去，就得到原方程的通解。为了减少运算次数，在用带余数除法时，我们总取绝对最小余数。如果不定方程无解，则在施行这种算法时，到某一步就会直接看出，下面来举一个例子。

例 4　求 $117x_1 + 21x_2 = 38$ 的解。

解

$$x_2 = \frac{1}{21}(-117x_1 + 38)$$

$$= -6x_1 + 2 + \frac{1}{21}(9x_1 - 4),$$

$$x_3 = \frac{1}{21}(9x_1 - 4) \in \mathbf{Z},$$

$$x_1 = \frac{1}{9}(21x_3 + 4)$$

$$= 2x_3 + \frac{1}{9}(3x_3 + 4),$$

$$x_4 = \frac{1}{9}(3x_3 + 4) \in \mathbf{Z},$$

$$x_3 = \frac{1}{3}(9x_4 - 4) = 3x_4 - 1 - \frac{1}{3}.$$

最后一式表明：x_3, x_4 不可能同时为整数，所以不定方程无解。

下面来举一个用这种算法解三元一次不定方程的例子。

例 5　求 $15x_1+10x_2+6x_3=61$ 的全部解。

解　x_3的系数的绝对值最小，我们把原方程化为

$$x_3=\frac{1}{6}(-15x_1-10x_2+61)$$

$$=-2x_1-2x_2+10+\frac{1}{6}(-3x_1+2x_2+1),$$

$$x_4=\frac{1}{6}(-3x_1+2x_2+1)\in\boldsymbol{Z}.$$

用类似办法得

$$x_2=\frac{1}{2}(6x_4+3x_1-1)$$

$$=3x_4+x_1+\frac{1}{2}(x_1-1),$$

$$x_5=\frac{1}{2}(x_1-1)\in\boldsymbol{Z}.$$

解得

$$x_1=1+2x_5,\quad x_5=0,\pm1,\pm2,\cdots.$$

反推上去依次解出

$$x_2=3x_4+x_1+x_5=1+3x_4+3x_5,$$
$$x_4,x_5=0,\pm1,\pm2,\cdots.$$
$$x_3=-2x_1-2x_2+10+x_4$$
$$=6-5x_4-10x_5,$$
$$x_4,x_5=0,\pm1,\pm2,\cdots.$$

这就得到了原不定方程的通解，其中含有两个参数 x_4,x_5。

下面的定理表明：一般的 k 元一次不定方程可化为解由 $k-1$ 个二元一次不定方程构成的方程组，且它的通解中恰有 $k-1$ 个参数。

定理3 设 $g_1=a_1$, $g_2=(g_1,a_2)=(a_1,a_2)$, $g_3=(g_2,a_3)=(a_1,a_2,a_3)$, $\cdots$, $g_k=(g_{k-1},a_k)=(a_1,\cdots,a_k)$。那么，不定方程(1)等价于下面的有 $2(k-1)$ 个整数变数 $x_1,\cdots,x_k,y_2,\cdots,y_{k-1}$, $k-1$ 个方程的不定方程组：

$$\begin{cases} g_{k-1}y_{k-1}+a_kx_k=c, \\ g_{k-2}y_{k-2}+a_{k-1}x_{k-1}=g_{k-1}y_{k-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ g_2y_2+a_3x_3=g_3y_3, \\ g_1x_1+a_2x_2=g_2y_2. \end{cases} \tag{6}$$

当方程(1)有解时，它的通解由有 $k-1$ 个参数的线性表达式给出。

证 先来证等价性。若 $x_1,\cdots,x_k$, $y_2,\cdots,y_{k-1}$ 是方程组(6)的解，则显见 $x_1,\cdots,x_k$ 是(1)的解。反之，若 $x_1,\cdots,x_k$ 是(1)的解，则取

$$y_j=\frac{1}{g_j}(a_1x_1+\cdots+a_jx_j),\quad 2\leqslant j\leqslant k-1,$$

显见，y_j 是整数，且 $x_1,\cdots,x_k$, $y_2,\cdots,y_{k-1}$ 是(6)的解。由定理1容易看出，方程组(6)的第一个方程和方程(1)一样，有解的充要条件是 $g_k|c$。而(6)的其余的方程，当把 y_j 看作参数(取整数值)时，每个变数为 y_{j-1}, x_j 的二元一次不定方程

$$g_{j-1}y_{j-1}+a_jx_j=g_jy_j \tag{7}$$

总是可解的①，这里 j 依此取 $k-1,\cdots,2$。一定可以找到 $y_{j-1}^{(0)}$, $x_j^{(0)}$ 使

$$g_{j-1}y_{j-1}^{(0)}+a_jx_j^{(0)}=g_j, \tag{8}$$

这样 $y_jy_{j-1}^{(0)},y_jx_j^{(0)}$ 就是(7)的一组特解，由定理2知，(7)的通解是

---

① 这里当 $j=2$ 时，规定 $x_1=y_1$。

$$y_{j-1}=y_j y_{j-1}^{(0)}+\frac{a_j}{g_j}t_{j-1},\quad x_j=y_j x_j^{(0)}-\frac{g_{j-1}}{g_j}t_{j-1},\tag{9}$$

$$t_{j-1}=0,\pm 1,\pm 2,\cdots\qquad(2\leqslant j\leqslant k-1).$$

当(1)有解，即 $g_k|c$ 时，方程组(6)的第一个方程可解，且由定理 2 知，其通解是($y_{k-1,0}, x_{k,0}$ 是一组特解)

$$y_{k-1}=y_{k-1,0}+\frac{a_k}{g_k}t_{k-1},\quad x_k=x_{k,0}-\frac{g_{k-1}}{g_k}t_{k-1},\tag{10}$$

$$t_{k-1}=0,\pm 1,\pm 2,\cdots.$$

式(10)已经给出了 y_{k-1} 和 x_k 的参数 t_{k-1} 的表达式① .由 y_{k-1} 的参数表达式及式(9) ($j=k-1$)可得到 y_{k-2} 和 x_{k-1} 的参数 t_{k-1}, t_{k-2} 的表达式；进而由 y_{k-2} 的参数表达式及式(9) ($j=k-2$)可得到 y_{k-3} 和 x_{k-2} 的参数 t_{k-1},t_{k-2},t_{k-3} 的表达式；依次就得到 y_{j-1} 和 x_j ($j=k-3,\cdots,2$)的参数 $t_{k-1},\cdots,t_{j-1}$ 的表达式。这就给出了方程组(6)变元 $x_1,\cdots,x_k$, $y_2,\cdots,y_{k-1}$ (注意 $x_1=y_1$)的通解公式(为什么)，其中有 $k-1$ 个参数 $t_1,\cdots,t_{k-1}$。显见，其中的一部分——$x_1,\cdots,x_k$ 的参数表示式就给出了不定方程(1)的通解公式(为什么)。证毕。

下面仍以例 5 为例，说明如何用定理 3 的方法来解 $k(>2)$ 元一次不定方程。

例 6 求 $15x_1+10x_2+6x_3=61$ 的解。

解 用定理 3 的方法来解。$a_1=15$, $a_2=10$, $a_3=6$。所以 $g_1=15$, $g_2=(15,10)=5$, $g_3=(5,6)=1$。因此这不定方程等价于 4 个变数，两个方程的不定方程组：

$$\begin{cases}5y_2+6x_3=61,\\15x_1+10x_2=5y_2.\end{cases}$$

$15x_1+10x_2=5y_2$ 的通解是

① 这里所说的参数表达式都是线性的，下同。

$$x_1 = y_2 + 2t_1,\quad x_2 = -y_2 - 3t_1,\quad t_1 = 0, \pm 1, \cdots.$$

$5y_2 + 6x_3 = 61$ 的通解是

$$y_2 = 5 + 6t_2,\quad x_3 = 6 - 5t_2,\quad t_2 = 0, \pm 1, \cdots.$$

消去 y_2 就得到原不定方程的通解：

$$x_1 = 5 + 2t_1 + 6t_2,\quad x_2 = -5 - 3t_1 - 6t_2,\quad x_3 = 6 - 5t_2,$$

$$t_1, t_2 = 0, \pm 1, \cdots.$$

比较得到的两个通解公式，可以发现含有的参数个数都是两个，但具体的表示形式却有很大不同，这是由于所用的解法不同引起的，而实质上是一样的。关于这一点将在习题中讨论。

定理 3 已经涉及比较简单的一次不定方程组的问题，对这一问题的讨论比较烦，要用到一些整数矩阵的知识，这里不作进一步讨论了。有兴趣的读者可参看文献[2],[4].

下面我们来讨论当二元一次不定方程(4)可解时，它的非负解和正解问题。由通解公式(5)知这可归结为去确定参数 t 的值，使 x_1, x_2 均为非负或正。显见，当 a_1, a_2 异号时，不定方程(4)可解时总有无穷多组非负解或正解。所以，只要讨论 a_1, a_2 均为正的情形。先来讨论非负解。

定理4 设 a_1, a_2 及 c 均为正整数，$(a_1, a_2) = 1$。那么，当 $c > a_1a_2 - a_1 - a_2$ 时，不定方程(4)有非负解，解数等于 $[c/(a_1a_2)]$ 或 $[c/(a_1a_2)] + 1$；当 $c = a_1a_2 - a_1 - a_2$ 时，不定方程(4)没有非负解。

证 由于 $(a_1, a_2) = 1$，所以方程(4)必有解。设 $x_{1,0}, x_{2,0}$ 是方程(4)的一组特解。由通解公式(5)知，所有非负解 x_1, x_2 由满足以下条件的参数 t 给出：

$$-x_{1,0}/a_2 \leqslant t \leqslant x_{2,0}/a_1,$$

由此及 $[x]$ 的定义、第一章 §8定理 1 (vii)知，上式即

$$-[x_{1,0}/a_2] \leqslant t \leqslant [x_{2,0}/a_1]. \tag{11}$$

因此，方程(4)的非负解的组数

$$N_0 = [x_{1,0}/a_2] + [x_{2,0}/a_1] + 1. \tag{12}$$

由此及第一章§8定理1(iv)推得

$$[x_{1,0}/a_2+x_{2,0}/a_1]\leqslant N_0\leqslant[x_{1,0}/a_2+x_{2,0}/a_1]+1,$$

且上式中等号有且仅有一个成立。由于 $x_{1,0},x_{2,0}$ 是特解，所以

$$x_{1,0}/a_2+x_{2,0}/a_1=c/(a_1a_2).$$

由以上两式得

$$N_0=[c/(a_1a_2)] \text{ 或 } [c/(a_1a_2)]+1.$$

当 $c>a_1a_2-a_1-a_2$ 时

$$\begin{aligned}1-1/a_1-1/a_2<c/a_1a_2&=x_{1,0}/a_2+x_{2,0}/a_1\\&=[x_{1,0}/a_2]+\{x_{1,0}/a_2\}+[x_{2,0}/a_1]+\{x_{2,0}/a_1\}\\&\leqslant[x_{1,0}/a_2]+[x_{2,0}/a_1]+(a_1-1)/a_1\\&\quad+(a_2-1)/a_2,\end{aligned}$$

最后一步用到了对正整数 n,m，必有 $\{m/n\}\leqslant(n-1)/n$。由此即得

$$[x_{1,0}/a_2]+[x_{2,0}/a_1]>-1,$$

进而由此及式(12)推出 $N_0>0$，即这时必有非负解。

当 $c=a_1a_2-a_1-a_2$ 时，若有非负解 x_1,x_2，则有

$$a_1(x_1+1)+a_2(x_2+1)=a_1a_2,\tag{13}$$

由此及 $(a_1,a_2)=1$，利用第一章§4定理11可得

$$a_1\mid x_2+1,\quad a_2\mid x_1+1.$$

由于 $x_1\geqslant0$，$x_2\geqslant0$，所以必有 $x_2+1\geqslant a_1\geqslant1$，$x_1+1\geqslant a_2\geqslant1$。由此及式(13)推出

$$a_1a_2\geqslant2a_1a_2.$$

但这是不可能的。所以，当 $c=a_1a_2-a_1-a_2$ 时，方程(4)没有非负解。定理证毕。

下面来讨论正解。

定理5 设 a_1,a_2 及 c 均为正整数，$(a_1,a_2)=1$。那么，当 $c>a_1a_2$ 时，方程(4)有正解，解数等于 $-[-c/(a_1a_2)]-1$ 或 $-[-c/(a_1a_2)]$；当 $c=a_1a_2$ 时，方程(4)无正解。

证 由于 $(a_1,a_2)=1$，方程(4)必有解。设 $x_{1,0},x_{2,0}$ 是方程(4)

的一组特解。由通解公式(5)知，所有正解x_1, x_2由满足以下条件的参数 t 给出

$$-x_{1,0}/a_2 < t < x_{2,0}/a_1,$$

由此及第一章 § 8定理 1 的(viii)和(ix)知，上式即

$$[-x_{1,0}/a_2]+1 \leqslant t \leqslant -[-x_{2,0}/a_1]-1. \tag{14}$$

因此，正解的组数

$$N_1 = -[-x_{1,0}/a_2]-[-x_{2,0}/a_1]-1. \tag{15}$$

由此及第一章 § 8定理 1 (iv)推得

$$-[-x_{1,0}/a_2 - x_{2,0}/a_1]-1 \leqslant N_1 \leqslant -[-x_{1,0}/a_2 - x_{2,0}/a_1].$$

由于 $x_{1,0}, x_{2,0}$ 是解，所以

$$-x_{1,0}/a_2 - x_{2,0}/a_1 = -c/(a_1a_2).$$

由以上两式即得

$$N_1 = -[-c/(a_1a_2)]-1 \text{ 或 } -[-c/(a_1a_2)].$$

当 $c > a_1a_2$ 时 $-[-c/(a_1a_2)] \geqslant 2$，因此 $N_1 \geqslant 1$即必有正解。当 $c = a_1a_2$ 时，若有正解 x_1, x_2，则有

$$a_1x_1 + a_2x_2 = a_1a_2, \tag{16}$$

由此及$(a_1, a_2)=1$，利用第一章 § 4定理11可得

$$a_2 \mid x_1, \quad a_1 \mid x_2.$$

由于 $x_1 \geqslant 1$，$x_2 \geqslant 1$，所以必有 $x_1 \geqslant a_2 \geqslant 1$，$x_2 \geqslant a_1 \geqslant 1$。由此及式(16)推出

$$a_1a_2 \geqslant 2a_1a_2.$$

但这是不可能的。所以当 $c = a_1a_2$ 时，方程(4)无正解。证毕。

应该指出：方程(4)有正解的充要条件是方程

$$a_1x_1 + a_2x_2 = c - a_1 - a_2$$

有非负解。因此，定理 4 和定理 5 只要证明了一个就能推出另一个，详细的论证留给读者。此外，这两个定理中的解数公式(12)和(15)在一些情况下比定理中的结论更有用，当然，这需要先找出一组特解(并不一定要是非负解或正解)。下面来举几个例。

例 7 求 $5x_1+3x_2=52$ 的全部正解。

解 $x_1=8$，$x_2=4$ 是一组特解，由式(5)和(14)知全部正解是：

$$x_1=8+3t,\quad x_2=4-5t,$$

$$-2=[-8/3]+1\leqslant t\leqslant -[-4/5]-1\leqslant 0.$$

所以共有三组正解：8,4；5,9；2,14。容易看出 $x_1=0$ 或 $x_2=0$ 都不可能是解，因此这也是全部非负解。

例 8 证明：$101x_1+37x_2=3189$ 有正整数解。

证 这里 $c=3189<a_1a_2=101\cdot 37$，所以从定理 5 的结论不能确定方程是否有正解(当然可推出至多有一个)。因此需要利用式(15)(或(14))。可以求出 $x_1=11\cdot 3189$，$x_2=-30\cdot 3189$ 是一组特解(请读者自己去求)，由式(15)知解数等于

$$-[-11\cdot 3189/37]-[30\cdot 3189/101]-1$$

$$=948-947-1=1.$$

即方程恰有一组正解。请读者自己去求出这组正解。

例 9 鸡翁一，值钱五，鸡母一，值钱三，鸡雏三值钱一。百钱买百鸡。问鸡翁母雏各几何？

解 以 x_1,x_2,x_3 分别代表鸡翁，鸡母，雏鸡的数目，由条件可得下面的不定方程组

$$\begin{cases} 5x_1+3x_2+x_3/3=100, \\ x_1+\ \ x_2+x_3=100. \end{cases}$$

我们要求这不定方程组的非负解。消去 x_3 可得

$$7x_1+4x_2=100.$$

先求这不定方程的非负解。$x_1=0$，$x_2=25$ 是一组特解。由式(5)及定理 4 知，它的全部非负解是：

$$x_1=0+4t,\quad x_2=25-7t,$$

$$0=-[0/4]\leqslant t\leqslant [25/7]=3.$$

即是 0,25；4,18；8,11；12,4。因此所买的鸡的各种可能的情形是下表：

x_1	0	4	8	12
x_2	25	18	11	4
x_3	75	78	81	84

例10 求 $15x_1+10x_2+6x_3=61$ 的全部非负解。

解 由例 6 知通解公式是

$$x_1=5+2t_1+6t_2,\quad x_2=-5-3t_1-6t_2,\quad x_3=6-5t_2.$$

所以给出非负解的 t_1,t_2 是

$$5+2t_1+6t_2\geqslant 0,\quad -5-3t_1-6t_2\geqslant 0,\quad 6-5t_2\geqslant 0.$$

由此得

$$-5/3-2t_2\geqslant t_1\geqslant -5/2-3t_2,\quad t_2\leqslant 6/5.$$

进而有

$$-5/6\leqslant t_2\leqslant 6/5.$$

所以，$t_2=0,1$。容易算出，$t_2=0$ 时，$t_1=-2$；$t_2=1$ 时，$t_1=-4,-5$。由此从通解公式求出所有非负解是：

$$1,1,6;\quad 3,1,1;\quad 1,4,1.$$

由例 5 所得的通解公式也可得到同样的结果。

习　题　一

1．求解以下方程：

(i) $3x_1+5x_2=11$；　(ii) $60x_1+123x_2=25$；

(iii) $903x_1+731x_2=1106$；　(iv) $21x_1+35x_2=98$；

(v) $1402x_1-1969x_2=2$。

2．求解以下方程：

(i) $x_1-2x_2-3x_3=7$；　(ii) $3x_1+6x_2-4x_3=7$；

(iii) $6x_1+10x_2-21x_3+14x_4=1$。

3. 求解不定方程组：

(i) $x_1+2x_2+3x_3=7$, $2x_1-5x_2+29x_3=11$;

(ii) $3x_1+7x_2=2$, $2x_1-5x_2+10x_3=8$;

(iii) $x_1^2+x_2^2=x_3^2$, $x_2=(x_1+x_3)/2$;

(iv) $x_1+x_2+x_3=94$, $x_1+8x_2+50x_3=87$;

(v) $x_1+x_2+x_3=99$, $x_1+6x_2+21x_3=100$;

(vi) $x_1+x_2+x_3+x_4=100$; $x_1+2x_2+3x_3+4x_4=300$, $x_1+4x_2+9x_3+16x_4=1000$.

4. 设$(a,b)=1$，c为整数。证明：在平面直角坐标系中以$ax+by=c$为方程的直线上，任一长度$\geqslant(a^2+b^2)^{1/2}$的线段上(包括端点）必有一点，其坐标为整数。

5. 证明：$a_1x_1+a_2x_2=c$的通解为$x_1=e+ft$，$x_2=g+ht$，$t=0,\pm1,\pm2,\cdots$(其中e,f,g,h为整数)的充要条件是$x_1=e,x_2=g$是解，以及$f=a_2/(a_1,a_2),h=-a_1/(a_1,a_2)$或$f=-a_2/(a_1,a_2)$，$h=a_1/(a_1,a_2)$。

6. 设$k<h$。我们把不定方程组：$a_{1j}x_1+\cdots+a_{kj}x_k=c_j$，$1\leqslant j\leqslant h$，写为矩阵形式：

$$A\begin{pmatrix}x_1\\ \vdots\\ x_k\end{pmatrix}=\begin{pmatrix}c_1\\ \vdots\\ c_h\end{pmatrix},$$

其中矩阵$A=(a_{ij})$是h行k列。设T是元素均为整数的k阶矩阵，行列式等于±1，以及$d_1,\cdots,d_k$是整数。再设

$$\begin{pmatrix}x_1\\ \vdots\\ x_k\end{pmatrix}=T\begin{pmatrix}y_1\\ \vdots\\ y_k\end{pmatrix}+\begin{pmatrix}d_1\\ \vdots\\ d_k\end{pmatrix}.$$

证明：原不定方程组有解的充要条件是：不定方程组

$$AT\begin{pmatrix}y_1\\ \vdots\\ y_k\end{pmatrix}=\begin{pmatrix}c_1\\ \vdots\\ c_h\end{pmatrix}-A\begin{pmatrix}d_1\\ \vdots\\ d_k\end{pmatrix}$$

有解。

7. 在§1定理3的符号下，证明：

(i) §1的不定方程(1)等价于不定方程组：

$$a_1x_1+a_2x_2=g_2y_2,\quad g_2y_2+a_3x_3+\cdots+a_kx_k=c;$$

(ii) 对任一取定的$2\leqslant h<k$，§1的不定方程(1)也等价于不定方程组：

$$a_1x_1+\cdots+a_hx_h=g_hy_h,\quad g_hy_h+a_{h+1}x_{h+1}+\cdots+a_kx_k=c;$$

(iii) $x_1,\cdots,x_k$ 是不定方程(1)的非负解（或正解）的充要条件是 $x_1,\cdots,x_k$，y_h 是(ii)中的不定方程组的非负解（或正解）；

(iv) $x_1,\cdots,x_k$ 是(1)的非负解（或正解）的充要条件是 $x_1,\cdots,x_k,y_2,\cdots,y_{k-1}$ 是定理3中的不定方程组的非负解（或正解）；

(v) 由(iv)提出一个求不定方程(1)的非负解（或正解）的方法，并用以求出§1例5的不定方程的全部非负解。

8. 求以下方程的全部非负解、全部正解。

(i) $5x_1+7x_2=41$；　　(ii) $96x_1+97x_2=1000$；

(iii) $7x_1+3x_2=123$；　　(iv) $15x_1+12x_2+20x_3=59$。

9. 有大学生、中学生和小学生共20人去公园，大学生门票每人3元，中学生每人2元，小学生每人5角。门票钱共20元，问大、中、小学生各有几人？

10. 有面值为1元、2元及5元的人民币共50张，为使它们的总值是100元，这些面值的人民币的张数可以如何选择。

11. 有甲、乙、丙三人共有100元钱。如果甲的钱变为原来的6倍，乙的钱变为原来的1/3，丙的钱不变，则三人仍然共有100元。丙的钱不多于30元。问甲、乙、丙各有多少钱？

12. 某人买了黑、白瓜子共12包，花了9元9角。每包白瓜子比黑瓜子贵3角，且白瓜子的包数比黑瓜子多。问黑、白瓜子各买了几包？

13. 有甲、乙两人分别拿了40个和30个鸡蛋到集市上去出售。开始他们都以5角一个出售，在各自出售了一些后，降低价格，

但仍都以同样的价格（每个若干角）出售。到鸡蛋全卖完时，他们发现所得的钱相同。问他们最多能得多少钱？最少能得多少钱？

14．甲班有儿童 7 人，乙班有10人。现有100个苹果分给甲、乙两班。问甲、乙两班要各分多少，才能使甲班的每个儿童分到的苹果一样多，乙班的每个儿童分到的苹果也一样多。

15．(i) 将分数23/30表为三个既约分数之和，它们的分母两两既约；

(ii) 将23/30表为两个既约分数之和，它们的分母既约。

16．有五个水手和一只猴子在一个小岛上，他们白天采集了一些椰子作为食物。晚上，一个水手醒了，决定拿出自己的一份椰子。他把椰子分为相等的五份后，还剩下一个，所以他把剩下的一个给了猴子，然后把自己的一份藏起来，就回去睡了。过了一会儿，第二个水手醒了，他和第一个一样，也决定拿出自己的一份。当他把剩下的椰子分为相等的五份后，也还剩下一个，他把这一个也给了猴子，然后把自己的一份藏起来，也回去睡了。剩下的三个水手也依次做了同样的事情，第二天早上，他们醒来后，都装得什么事也没有发生一样，把剩下的椰子分为相等的五份，一人一份，这次一个也没有剩下。问：原来这堆椰子最少有多少，他们每人总共拿到了多少椰子？

17．求以下不定方程组的全部正解：

(i) $2x_1+x_2+x_3=100$，　$3x_1+5x_2+15x_3=270$；

(ii) $x_1+x_2+x_3=31$，　$x_1+2x_2+3x_3=41$。

18．将定理 4 、定理 5 推广到$(a_1,a_2)=g>1$的情形。

19．详细写出：(i) 由定理 4 成立推出定理 5 的证明；

(ii) 由定理 5 成立推出定理 4 的证明。

20．$63x_1+110x_2=6893$有无正解？

21．设 a_1,a_2,c 是正整数，$(a_1,a_2)=1$。对于方程$a_1x_1+a_2x_2=c$ 有以下结论：(i) $c<a_1+a_2$ 时一定没有正解；(ii) 全体非负解和全体正解相同的充要条件是$a_1\nmid c$ 且 $a_2\nmid c$；(iii) 若 $a_1|c$，

$a_1a_2 \nmid c$，则正解的个数等于$[c/(a_1a_2)]$；（iv）若$a_1a_2|c$，则正解个数等于$-1+c/(a_1a_2)$。

22．设a_1, a_2, a_3是两两既约的正整数。证明：不定方程$a_2a_3x_1+a_3a_1x_2+a_1a_2x_3=c$，当$c>2a_1a_2a_3-a_1a_2-a_2a_3-a_3a_1$时一定有非负解；当$c=2a_1a_2a_3-a_1a_2-a_2a_3-a_3a_1$时无非负解。

23．设n是正整数。证明：不定方程$x_1+2x_2+3x_3=n$的非负解的个数等于有理函数$(1-y)^{-1}(1-y^2)^{-1}(1-y^3)^{-1}$的幂级数展开式中$y^n$的系数。你会求出这个系数吗？如何把这方法推广，去求不定方程$a_1x_1+\cdots+a_kx_k=n$的非负解个数，这里$a_1,\cdots,a_k,n$是正整数。如果要求正解的个数，以上的方法要作怎样改变。

§ 2 $x^2+y^2=z^2$

这一节讨论二次不定方程

$$x^2+y^2=z^2. \tag{1}$$

方程(1)满足$xyz=0$的解称为显然解，$xyz\neq 0$的解称为非显然解。容易看出，全体显然解是

$$0, \pm a, \pm a;\quad \pm a, 0, \pm a,\quad a\geqslant 0, \tag{2}$$

这里正负号任意选取。若x, y, z是(1)的非显然解，那么，对任意正整数k，$\pm kx, \pm ky, \pm kz$（正负号任选）也是(1)的非显然解；以及对x, y, z的任意的正公约数d，$\pm x/d, \pm y/d, \pm z/d$（正负号任选）也是(1)的非显然解。因此，为了求出全部非显然解，只要求方程(1)满足以下条件的解：

$$x>0, y>0, z>0, (x, y, z)=1, \tag{3}$$

即既约的正解x, y, z，这样的解称为方程(1)的**本原解**。

引理1 不定方程(1)的本原解x, y, z必满足条件：

$$(x, y)=(y, z)=(z, x)=1, \tag{4}$$

$$2\nmid x+y. \tag{5}$$

证 若x, y不既约，则有素数$p|x, p|y$，由(1)知$p|z^2$。由

此及第一章§6定理1知 $p|z$。但这和 $(x,y,z)=1$ 矛盾。同理证 $(y,z)=1$，$(z,x)=1$。由 $(x,y)=1$ 知，x,y 不能同为偶数。x,y 也不能同为奇数。因为若同为奇数，则可推出 $4\nmid x^2+y^2$ 及 z 为偶数。而由(1)知

$$4\mid z^2=x^2+y^2,$$

矛盾。所以 x,y 必为一奇一偶，即式(5)成立。

定理2 不定方程(1)的 y 为偶数的全体本原解由以下公式给出：

$$x=r^2-s^2,\quad y=2rs,\quad z=r^2+s^2,\tag{6}$$

其中 r,s 为满足以下条件的任意整数：

$$r>s>0,\quad (s,r)=1,\quad 2\nmid r+s.\tag{7}$$

证 先证由式(6)，(7)给出的 x,y,z 一定是(1)的本原解且 $2|y$。容易验证：对任意的 r,s（不一定满足(7)），由式(6)给出的 x，y,z 一定是(1)的解且 $2|y$。由 $r>s>0$ 知，这是正解。由式(6)知

$$(x,z)\mid 2r^2,\quad (x,z)\mid 2s^2.$$

由此从第一章§4定理7和定理8推出

$$(x,z)\mid(2r^2,2s^2)=2(r^2,s^2).$$

由条件 $(s,r)=1$ 及第一章§4定理10推出 $(r^2,s^2)=1$。因而

$$(x,z)\mid 2.$$

由条件 $2\nmid r+s$ 知 $2\nmid x$，所以必有 $(x,z)=1$。这就证明了所要的结论。

下面来证：方程(1)的每一组本原解 $x,y,z,2|y$，一定可以表为式(6)的形式，且 r,s 满足式(7)。由引理1知 $2\nmid x+y$，由此及 $2|y$ 推出 $2\nmid x,2\nmid z$。因而有

$$\left(\frac{y}{2}\right)^2=\frac{z+x}{2}\cdot\frac{z-x}{2}.\tag{8}$$

由引理1知 $(x,z)=1$。由此及

$$\left(\frac{z+x}{2},\frac{z-x}{2}\right)\Big|\,x,\quad \left(\frac{z+x}{2},\frac{z-x}{2}\right)\Big|\,z$$

推出

$$\left(\frac{z+x}{2},\frac{z-x}{2}\right)=1.$$

利用第一章§6推论5（或§4例6），由上式及式(8)得

$$\frac{z+x}{2}=r^2,\quad \frac{z-x}{2}=s^2,$$

这里 r,s 是两个正整数，$r>s$ 且 $(r,s)=1$。从上式及式(8)立即推出式(6)成立。进而由 $2\nmid x$ 知 $2\nmid r+s$。这就证明了所要的结论。定理证毕。

从定理2及一开始的讨论就可以得到(1)的全部解：显然解由式(2)给出，非显然解是

$$x=\pm k(r^2-s^2),\quad y=\pm 2ksr,\quad z=\pm k(r^2+s^2),\tag{9}$$

及

$$x=\pm 2ksr,\quad y=\pm k(r^2-s^2),\quad z=\pm k(r^2+s^2),\tag{10}$$

其中 r,s 满足式(7)，k 是任意正整数，正负号任意选取。显见，全取正号及 $k=1$，就给出了全部本原解。

我们知道，一个直角三角形斜边长度的平方等于两直角边的长度平方之和。这就是著名的商高定理①。这样，求不定方程(1)的正整数解的几何意义就是要求边长为整数的直角三角形，这种三角形称为商高三角形②。当商高三角形的三边长为既约（即相应于(1)的本原解）时，称为**本原商高三角形**。定理2也就是求出了所有的本原商高三角形。

我们还可以从另一角度来看不定方程(1)的几何意义。方程(1)的解 x,y,z，当 $z=0$ 时，必有 $x=y=0$。我们约定只考虑(1)的 $z\neq0$ 的解。设

$$\xi=x/z,\quad \eta=y/z.\tag{11}$$

这样，方程(1)就变为

$$\xi^2+\eta^2=1.\tag{12}$$

---

① 亦称为毕达哥拉斯定理。

② 亦称为毕达哥拉斯三角形。

不定方程(1)的求解问题（注意 $z\neq0$）就等价于求方程(12)的有理数解 ξ,η。在直角坐标平面上，方程(12)表示单位圆周（这是二次曲线），因此，求方程(12)的有理数解就是求单位圆周上坐标为有理数的点，即**有理点**。由前面的讨论立即得到

推论3 单位圆周上的整点是：

$$\{\pm1,0\},\quad\{0,\pm1\};$$

不是整点的有理点是：

$$\left\{\pm\frac{r^2-s^2}{r^2+s^2},\pm\frac{2sr}{r^2+s^2}\right\},\quad\left\{\pm\frac{2sr}{r^2+s^2},\pm\frac{r^2-s^2}{r^2+s^2}\right\},$$

其中 r,s 满足式(7)，正负号任意选取。

例1 求出 $r\leqslant7$ 时，由式(6)和(7)给出的全部本原解。

表 1

s \ r	2	3	4	5	6	7
1	3,4,5		15,8,17		35,12,37	
2		5,12,13		21,20,29		45,28,53
3			7,24,25			
4				40,9,41		33,56,65
5					11,60,61	
6						13,84,85

表1就给出了全部要求的本原解。

例2 求 $z=65$ 的不定方程(1)的全部解。

解 显然解是 $x=\pm65,y=0$；$x=0,y=\pm65$。为求非显然解，由式(9)和(10)知，先要把65表为

$$65=k(r^2+s^2),$$

其中 r,s 满足式(7)，$k\mid65,0<k<65$。k 可取1,5,13。当 $k=1$ 时，

$$65=8^2+1^2=7^2+4^2,$$

即 $r=8, s=1$； $r=7, s=4$，相应的解为

$$x=\pm 63,\ y=\pm 16;\quad x=\pm 33,\ y=\pm 56$$

及

$$x=\pm 16,\ y=\pm 63;\quad x=\pm 56,\ y=\pm 33.$$

当 $k=5$ 时，

$$65=5\cdot 13=5(3^2+2^2),$$

即 $r=3, s=2$，相应的解为

$$x=\pm 25,\ y=\pm 60\ \text{及}\ x=\pm 60,\ y=\pm 25.$$

当 $k=13$ 时，

$$65=13\cdot 5=13(2^2+1^2),$$

即 $r=2, s=1$，相应的解为

$$x=\pm 39,\ y=\pm 52\ \text{及}\ x=\pm 52,\ y=\pm 39.$$

这就求出了全部解．本原解仅有

$$63,16,65;\quad 33,56,65$$

及

$$16,63,65;\quad 56,33,65.$$

例 3 设 x,y,z 是(1)的解．证明：(i) $3|x, 3|y$ 至少有一个成立；(ii) $5|x, 5|y, 5|z$ 至少有一个成立．

证 只要对 x,y,z 是本原解来证明（为什么），不妨设由式(6)给出．若 $3\nmid y$ 则 $3\nmid r, 3\nmid s$．因此必有

$$r=3k\pm 1,\quad s=3h\pm 1.$$

不论何种情形均有 $3|x=r^2-s^2$．这就证明了(i)．若 $5\nmid y$ 则 $5\nmid r$，$5\nmid s$．因此必有

$$r=5k\pm 1,\quad 5k\pm 2,\quad s=5h\pm 1, 5h\pm 2.$$

当 $r=5k\pm 1, s=5h\pm 1$ 或 $r=5k\pm 2, s=5h\pm 2$ 时必有

$$5|x=r^2-s^2.$$

当 $r=5k\pm 1, s=5h\pm 2$ 或 $r=5k\pm 2, s=5h\pm 1$ 时必有

$$5|z=r^2+s^2.$$

由例 1 的表 1 可看出各种情形都能出现。此外，总有$4|x$或$4|y$成立。

利用定理 2 的方法与结果可以解决一类不定方程的求解问题。下面来证明两个定理。

定理4 不定方程

$$x^4+y^4=z^2 \tag{13}$$

无 $xyz\neq 0$的解。

证 显见，只要证明方程(13)无正整数解。用反证法。假若(13)有正整数解，那么在全体正整数解中，必有一组解x_0,y_0,z_0，使得 z_0 取最小值。我们要由此找出一组正整数解x_1,y_1,z_1，满足$z_1<z_0$，得出矛盾①。

(i) 必有$(x_0,y_0)=1$。若不然，就有素数 $p|x_0,p|y_0$。由此及$x_0^4+y_0^4=z_0^2$推出 $p^4|z_0^2,p^2|z_0$。因此，$x_0/p_0,y_0/p_0,z_0/p^2$ 也是(13)的正整数解，这和 z_0 的最小性矛盾。因此，x_0^2,y_0^2,z_0 是方程(1)的本原解。由引理知，x_0,y_0 必为一奇一偶，不妨设 $2|y_0$，以及$(z_0,y_0)=1$。

(ii) $g_1=(z_0-y_0^2,z_0+y_0^2)=1$. 因为 $g_1|(2z_0,2y_0^2)=2(z_0,y_0^2)=2$，由此及 $2\nmid z_0-y_0^2$ 即得 $g_0=1$。由此及由式(13)推出的

$$(z_0-y_0^2)(z_0+y_0^2)=x_0^4,$$

利用第一章§6推论5得到：

$$z_0-y_0^2=u^4,\quad z_0+y_0^2=v^4,$$

这里 $v>u>0,(u,v)=1,2\nmid uv$。进而有

$$y_0^2=(v^2-u^2)\frac{(v^2+u^2)}{2}. \tag{14}$$

(iii) $g_2=(v^2-u^2,(v^2+u^2)/2)=1$。因为

$$g_2|(v^2-u^2,v^2+u^2)|(2v^2,2u^2)=2(u^2,v^2)=2.$$

由$2\nmid uv$ 可推出 $2\nmid(u^2+v^2)/2$，因此 $g_2=1$。利用第一章§6

① 下面论证中用到第一章中的整除性质时，不再一一说明了。

推论 5，由此及式(14)得到

$$v^2 - u^2 = a^2, \quad (v^2 + u^2)/2 = b^2, \tag{15}$$

这里 $a>0, b>0, (a,b)=1$，及 $2|a, 2\nmid b$。

(iv) 由 u,v 满足的条件及式(15)推得：

$$0<b<v<z_0,$$

及 u,a,v 是方程(1)的本原解且 $2|a$。因此由定理 2 知：必有 r,s 满足式(7)使得

$$u=r^2-s^2, \quad a=2rs, \quad v=r^2+s^2.$$

由此及式(15)的第二式即得

$$r^4+s^4=b^2.$$

这表明 r,s,b 是方程(13)的正整数解，且有 $b<z_0$，这和 z_0 最小性矛盾。所以(13)无正整数解。证毕。

证明定理 4 的方法通常称为 Fermat **无穷递降法**。定理 4 的几何意义是：不存在直角边长均为平方数的商高三角形。由定理 4 立即推出

推论5 不定方程

$$x^4+y^4=z^4$$

无 $xyz\neq0$ 的解。

数学中一个未解决的著名问题是：当 $n\geqslant3$时，不定方程

$$x^n+y^n=z^n$$

无 $xyz\neq0$ 的整数解。这通常称为 Fermat Last Theorem。这是因为 Fermat 不加证明地提出了许多数论中的定理，这就是其中的一个。后来，大多数结论被证明是对的，个别的则被否定了。而最后唯有这一个"定理"既没有被证明也没有被否定。推论 5 表明当 $n=4$ 时结论是正确的。关于这问题已经得到了许多结论，但这些讨论已远远超出了本书的范围，在第六章 § 5将证明 $n=3$ 时结论也成立。

定理6 不定方程

$$x^2+y^2=z^4 \tag{16}$$

的满足条件$(x,y)=1$的全部正整数解是

$$x=|6a^2b^2-a^4-b^4|,y=4ab(a^2-b^2),z=a^2+b^2, \quad (17)$$

及

$$x=4ab(a^2-b^2),\quad y=|6a^2b^2-a^4-b^4|,\quad z=a^2+b^2, \quad (18)$$

其中 a,b 为满足以下条件的任意整数：

$$a>b>0,\quad (a,b)=1,\quad 2\nmid a+b. \quad (19)$$

证 设 x,y,z 是(16)的正整数解，满足$(x,y)=1$。因此，x，y,z^2 是方程(1)的本原解。由引理 1 知，x,y 为一奇一偶，不妨设$2|y$。由定理 2 知，必有

$$x=r^2-s^2,\quad y=2rs,\quad z^2=r^2+s^2, \quad (20)$$

其中 r,s 满足式(7)。因而 r,s,z 也是方程(1)的本原解。若$2|s$，则由定理 2 知

$$r=a^2-b^2,\quad s=2ab,\quad z=a^2+b^2, \quad (21)$$

其中 a,b 满足（注意 $r>s$）

$$a>b>0,\ (a,b)=1,\ 2\nmid a+b,\ a^2-b^2>2ab. \quad (22)$$

由式(20),(21)得

$$x=a^4+b^4-6a^2b^2,\ y=4ab(a^2-b^2),\ z=a^2+b^2. \quad (23)$$

由式(22)得

$$(\sqrt{2}-1)a>b>0,\ (a,b)=1,\ 2\nmid a+b. \quad (24)$$

若$2|r$，则由定理 2 知

$$r=2ab,\ s=a^2-b^2,\ z=a^2+b^2, \quad (25)$$

其中 a,b 满足（注意 $r>s$）

$$a>b>0,\ (a,b)=1,\ 2\nmid a+b,\ 2ab>a^2-b^2. \quad (26)$$

由式(20),(25)得

$$x=6a^2b^2-a^4-b^4,\ y=4ab(a^2-b^2),\ z=a^2+b^2. \quad (27)$$

由式(26)得

$$a>b>(\sqrt{2}-1)a>0,\ (a,b)=1,\ 2\nmid a+b. \quad (28)$$

由式(23),(27)及式(24),(28)推出：当$2|y$时，解由式(17),(19)给出。由对称性推出，当$2|x$时，解由式(18),(19)给出。此外，容易直接验证：由式(17),(18),(19)给出的x,y,z一定是方程(16)满足$(x,y)=1$的解。定理证毕。

习 题 二

1．求出不定方程$x^2+y^2=z^2$满足$|z|\leqslant 50$的全部解、正解、及本原解。

2．求出一边长为(i) 15；(ii) 22；(iii) 50的所有商高三角形、所有本原商高三角形。

3．对怎样的正整数n，不定方程$x^2-y^2=n$ (i) 有解；(ii) 有满足$(x,y)=1$的解。并对$n=30,60,120$判断这方程是否有解；有解时求出它的全部解，及全部满足$(x,y)=1$的解。进而，提出一个求解这不定方程的方法。

4．证明：(i) $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$；(ii) $(a^2-b^2)(c^2-d^2)=(ac+bd)^2-(ad+bc)^2$。

5．求出斜边为(i) 1105；(ii) 5525；(iii) 117；(iv) 351的所有商高三角形、所有本原商高三角形。

6．设$n\geqslant 3$。证明：必有一个商高三角形以n为其一直角边的长度。

7．求面积等于(i) 78；(ii) 360的所有商高三角形。

8．证明：对任意整数n，不定方程$x^2+y^2-z^2=n$一定可解。

9．证明：不定方程$x^2+2y^2=z^2$满足$(x,y,z)=1$的全部正解是：$x=|u^2-2v^2|,y=2uv,z=u^2+2v^2$，其中$u,v$是满足$(u,v)=1,2\nmid u$的任意正整数。

10．求$x^4+y^2=z^2$满足$(x,y)=1$的全部解。

11．求$x^2+3y^2=z^2$满足$(x,y)=1$的全部解。

12．证明：不定方程$1/x^2+1/y^2=1/z^2$的解一定满足

(i) $(x,y)>1$;　　(ii) $60\mid xy$;

(iii) 所有$(x,y,z)=1$的正解是：

$$x=r^4-s^4,\ \ y=2rs(r^2+s^2),\ \ z=rs(r^2-s^2),$$

其中 $r>s>0,(r,s)=1,2\mid rs$，以及交换x,y。

13．设$4\mid n>0$。证明：$x^n+y^n=z^n$ 无 $xyz\neq0$的解。

14．证明：$x^4+4y^4=z^2$ 无 $xyz\neq0$的解。

15．证明：$x^4+y^2=z^4$ 无 $xyz\neq0$的解。

16．证明：不定方程组 $x^2+y^2=z^2,x^2-y^2=w^2$无正整数解。

17．证明以上三题中的不定方程和不定方程组两两等价。

18．证明：商高三角形的面积一定不是整数的平方。

19．证明：$x^4-4y^4=z^2$ 无 $xyz\neq0$的解。

20．证明：上题中的不定方程和 $x^4+y^4=z^2$ 等价。

21．证明：不定方程 $w^2+x^2+y^2=z^2$ 的任一组解中，w,x,y 至少有两个是偶数。进而证明：这方程的 x,y 为偶数的通解是：

$$w=(l^2+m^2-n^2)/n,x=2l,y=2m,z=(l^2+m^2+n^2)/n,$$

其中 n,m,l 为任意整数，满足 $n\mid l^2+m^2$。

22．证明：不定方程 $x^n+y^n=z^{n+1}$有无穷多组解。

23．证明：不定方程 $x^n+y^n=z^{n-1}$有无穷多组解。

24．证明：不定方程 $x^2-2y^4=1$无正整数解。

25．证明：不定方程 $x^4-2y^2=-1$，除 $x=y=1$外，无其它正整数解。

26．证明：不定方程 $x^2-8y^4=1$，除 $x=3,y=1$外，无其它正整数解。

第三章　同　　余

本章将讨论有关同余理论的基本概念及基本性质．这些基本概念就是：同余，同余式，同余类，完全剩余系及既约剩余系．在§1中讨论同余与同余式的基本性质；在§2中讨论同余类与剩余系的基本性质，着重讨论它们的整体性质，不同模的同余类、剩余系之间的关系，这对理解与掌握同余理论是十分重要的；§3讨论模 m 的既约剩余系的元素个数 $\phi(m)$——Euler函数——的基本性质，这是一个十分重要的数论函数；最后在§4中讨论模 m 的一个既约剩余系中所有数的乘积对模 m 的剩余，即 Wilson 定理．

§1　同　　余

定义1（同余） 设 $m\neq 0$．若 $m\mid a-b$，即 $a-b=km$，则称 a **同余于 b 模 m，b 是 a 对模 m 的剩余**，记作

$$a\equiv b(\bmod m);\tag{1}$$

不然，则称 **a 不同余于 b 模 m，b 不是 a 对模 m 的剩余**，记作

$$a\not\equiv b(\bmod m).$$

关系式(1)称为**模 m 的同余式**，或简称**同余式**．

由于 $m\mid a-b$ 等价于 $-m\mid a-b$，所以同余式（1）等价于

$$a\equiv b(\bmod(-m)),$$

因此，以后总假定模 $m\geqslant 1$．在同余式(1)中，若 $0\leqslant b<m$，则称 **b 是 a 对模 m 的最小非负剩余**；若 $1\leqslant b\leqslant m$，则称 **b 是 a 对模 m 的最小正剩余**；若 $-m/2<b\leqslant m/2$（或 $-m/2\leqslant b<m/2$），则称 **b 是 a 对模 m 的绝对最小剩余**．

这样，$m|a$ 就可记为 $a\equiv 0(\bmod m)$，所以，所有的偶数可表为 $a\equiv 0(\bmod 2)$。由于奇数 a 满足 $2|a-1$，所以，所有的奇数可表为 $a\equiv 1(\bmod 2)$。对给定的 b 和模 m，所有同余于 b 模 m 的数就是算术数列

$$b+km, \quad k=0,\pm 1,\pm 2,\cdots.$$

定理1 a 同余于 b 模 m 的充要条件是 a 和 b 被 m 除后所得的最小非负余数相等，即若

$$a=q_1m+r_1, \quad 0\leqslant r_1<m;$$
$$b=q_2m+r_2, \quad 0\leqslant r_2<m,$$

则 $r_1=r_2$。

证 我们有 $a-b=(q_1-q_2)m+(r_1-r_2)$。因此，$m|a-b$ 的充要条件是 $m|r_1-r_2$，由此及 $0\leqslant|r_1-r_2|<m$ 即得 $r_1=r_2$。

"同余"按其词意来说，就是"余数相同"，定理 1 正好说明了这一点。容易证明（留给读者）：a 对模 m 的最小非负剩余、最小正剩余、及绝对最小剩余正好分别是 a 被 m 除后所得的最小非负余数、最小正余数、及绝对最小余数（见第一章 §3定理 2 后）。同余式(1) 就是一般的带余数除法

$$a=km+b. \tag{2}$$

我们知道，若式(2) 成立，那么在讨论一个 a 的多项式被 m 去除的问题时，b 与 a 是一样的，即 a 可用 b 代替，而其中的"部分商" k 不起作用。同余式符号 (1) 正是抓住了这一关键；在上面的除法算式中去掉了 k，保留了 b，突出了 a 与 b 在讨论被 m 整除的问题中两者起相同的作用。应用同余式的符号在讨论整除问题中，确实比应用整除符号及除法算式方便、有效，能起到旧有符号起不到的作用。这将在以后的讨论，及与第一章中的论证的比较来看出。为了学会应用这一新的符号，首先要来讨论它的基本性质。

对固定的模 m，同余、同余式和相等、等式有以下同样的性质：

性质 I 同余是一种等价关系，即有

$$a\equiv a\pmod m,$$

$$a\equiv b\pmod m\Longleftrightarrow b\equiv a\pmod m,$$

$$a\equiv b\pmod m,\ b\equiv c\pmod m\Longrightarrow a\equiv c\pmod m.$$

证 由 $m\mid a-a=0$， $m\mid a-b\Longleftrightarrow m\mid b-a$， 以及 $m\mid a-b$，$m\mid b-c\Longrightarrow m\mid(a-b)+(b-c)=a-c$，就推出这三个性质。

性质 II 同余式可以相加，即若有

$$a\equiv b\pmod m,\qquad c\equiv d\pmod m,\tag{3}$$

则

$$a+c\equiv b+d\pmod m.$$

证 由 $m\mid a-b$，$m\mid c-d\Longrightarrow m\mid(a-b)+(c-d)=(a+c)-(b+d)$，就证明了所要结论。

性质 III 同余式可以相乘，即若式（3）成立，则有

$$ac\equiv bd\pmod m.$$

证 由 $a=b+k_1m$，$c=d+k_2m$ 推出

$$ac=bd+(bk_2+dk_1+k_1k_2m)m,$$

这就证明了所要的结论。

由性质 I，II，III 立即推出（证明留给读者）：

性质 IV 设 $f(x)=a_nx^n+\cdots+a_0$，$g(x)=b_nx^n+\cdots+b_0$ 是两个整系数多项式，满足

$$a_j\equiv b_j\pmod m,\qquad 0\leqslant j\leqslant n.\tag{4}$$

那么，若 $a\equiv b\pmod m$，则

$$f(a)\equiv g(b)\pmod m.$$

通常我们把满足条件（4）的这两个多项式 $f(x)$，$g(x)$ 称为多项式 $f(x)$ 同余于多项式 $g(x)$ 模 m，记作

$$f(x)\equiv g(x)\pmod m.\tag{5}$$

应该指出的是：对所有的整数 x 有

$$f(x)\equiv g(x)\pmod m\tag{6}$$

成立时，并不一定有式（5）成立。例如，对所有整数 x 有

$$x(x-1)\cdots(x-m+1)\equiv 0(\bmod m)$$

成立；由第一章§4例3(ii)知，当 $m=$ 素数 p 时，对所有整数 x 有

$$x^p-x\equiv 0(\bmod p)$$

成立。但是，显然有

$$x(x-1)\cdots(x-m+1)\not\equiv 0(\bmod m),$$

$$x^p-x\not\equiv 0(\bmod p)。$$

对所有整数 x 都成立的同余式(6)称为是模 m **的恒等同余式**。显见，式(5)一定是恒等同余式，但上面两例表明反过来并不一定对。

下面是涉及模的两个简单性质。

性质Ⅴ 设 $d\geqslant 1$，$d\mid m$。那么，若同余式(1)成立，则

$$a\equiv b(\bmod d)。$$

证 这由 $d\mid m$，$m\mid a-b\Longrightarrow d\mid a-b$ 即得。

性质Ⅵ 设 $d\neq 0$。那么同余式（1）等价于

$$da\equiv db(\bmod |d|m)。$$

证 这由 $|d|m\mid da-db\Longleftrightarrow m\mid a-b$ 推出。

一般说来，在模不变的条件下，同余式两边不能相约，即由 $d\neq 0$，$da\equiv db(\bmod m)$ 不能推出必有 $a\equiv b(\bmod m)$。例如：$6\cdot 3\equiv 6\cdot 8(\bmod 10)$，但 $3\not\equiv 8(\bmod 10)$。以上的性质仅是最简单的整除性质（第一章§2定理1）用同余符号相表示。由进一步的整除性质可得到相应的同余式的性质，这些性质和等式性质不同。

性质Ⅶ 同余式

$$ca\equiv cb(\bmod m) \tag{7}$$

等价于

$$a\equiv b(\bmod m/(c,m))。$$

特别地，当 $(c,m)=1$ 时，同余式(7)等价于

$$a\equiv b(\bmod m),$$

即同余式（7）两边可约去 c。

证 同余式（7）即 $m\mid c(a-b)$，这等价于

$$\frac{m}{(c,m)}\Big|\frac{c}{(c,m)}(a-b).$$

由第一章§4定理11及 $(m/(c,m),c/(c,m))=1$知，这等价于

$$\frac{m}{(c,m)}\Big|a-b.$$

这就证明了所要的结论。

性质Ⅷ 若 $m\geqslant 1$，$(a,m)=1$，则存在 c 使得

$$ca\equiv 1(\bmod m). \tag{8}$$

我们把 c 称为是 **a 对模 m 的逆**，记作 $a^{-1}(\bmod m)$或 a^{-1}。

证 由第一章§4定理13($k=2$)知，存在 x_0,y_0，使得 $ax_0+my_0=1$。取 $c=x_0$ 即满足要求。

例如

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

(mod 7)

a	1	5	7	11
a^{-1}	1	5	7	11

(mod 12)

a	1	2	3	4	5	6	7	8	9	10	11	12
a^{-1}	1	7	9	10	8	11	2	5	3	4	6	12

(mod 13)

显见，a 对模 m 的逆 c 不是唯一的。当 c 是 a 对模 m 的逆时，任一 $\tilde{c}\equiv c(\bmod m)$ 也一定是 a 对模 m 的逆；以及由性质Ⅶ知，a 对模 m 的任意两个逆 c_1,c_2 必有 $c_1\equiv c_2(\bmod m)$。以后我们写 $a^{-1}(\bmod m)$或 a^{-1}时是指任一取定的满足式(8)的 c。此外，显见 $(a^{-1},m)=1$ 及 $(a^{-1})^{-1}\equiv a(\bmod m)$。

性质Ⅸ 同余式组

$$a\equiv b(\bmod m_j),\quad j=1,2,\cdots,k$$

同时成立的充要条件是

$$a\equiv b(\bmod[m_1,\cdots,m_k]).$$

证 由第一章§1定理6知，$m_j|a-b$ $(j=1,\cdots,k)$ 同时成立的充要条件是$[m_1,\cdots,m_k]|a-b$。这就是要证的结论。

由于同余式有以上这些性质，特别是有类似于等式的性质使得我们在解整除问题时，利用同余符号比利用整除符号要方便得多。下面来举几个例子。

例1 求3^{406}写成十进位数时的个位数。

按题意是要求a满足

$$3^{406}\equiv a(\bmod 10),\quad 0\leqslant a\leqslant 9.$$

显然有，$3^2\equiv 9\equiv -1(\bmod 10)$，$3^4\equiv 1(\bmod 10)$. 进而有$3^{404}\equiv 1(\bmod 10)$。因此，$3^{406}\equiv 3^{404}\cdot 3^2\equiv 9(\bmod 10)$。所以个位数是9。

例2 求3^{406}写成十进位数时的最后两位数。

我们只要求出b满足

$$3^{406}\equiv b(\bmod 100),\quad 0\leqslant b\leqslant 99.$$

注意到$100=4\cdot 25$，$(4,25)=1$。显然有$3^2\equiv 1(\bmod 4)$，$3^4\equiv 1(\bmod 5)$。注意到4是最小的方次，由第一章§4例7知，使$3^d\equiv 1(\bmod 25)$成立的d，必有$4|d$。因此计算：

$$3^4\equiv 81\equiv 6(\bmod 25),\quad 3^8\equiv 36\equiv 11(\bmod 25),$$
$$3^{12}\equiv 66\equiv -9(\bmod 25),\quad 3^{16}\equiv -54\equiv -4(\bmod 25),$$
$$3^{20}\equiv -24\equiv 1(\bmod 25).$$

由此及$3^{20}\equiv 1(\bmod 4)$，从性质Ⅸ推出$3^{20}\equiv 1(\bmod 100)$，$3^{400}\equiv 1(\bmod 100)$。因此，$3^{406}\equiv 3^{400}\cdot 3^6\equiv 3^6\equiv 29(\bmod 100)$。所以，个位数为9，十位数为2。

如果不利用性质$4|d$，就要逐个计算3^j对模25的剩余b_j（为便于计算b_j应取绝对最小剩余），具体做法如下表：

j	1	2	3	4	5	6	7	8	9	10
b_j	3	9	2	6	−7	4	12	11	8	−1

由这里得到的 $3^{10}\equiv -1 \pmod{25}$ 就推出 $3^{20}\equiv 1 \pmod{25}$。

例 3　证明$641 \mid 2^{2^5}+1$。

由于数目很大要直接用除法做是很繁的。利用同余式就是要证$2^{32}\equiv -1 \pmod{641}$。641是素数，由逐步计算得：

$2^9\equiv 512\equiv -129 \pmod{641}$，$2^{11}\equiv -516\equiv 125 \pmod{641}$，

$2^{13}\equiv 500\equiv -141 \pmod{641}$，$2^{15}\equiv -564\equiv 77 \pmod{641}$，

$2^{18}\equiv 616\equiv -25 \pmod{641}$，$2^{22}\equiv -400\equiv 241 \pmod{641}$，

$2^{23}\equiv 482\equiv -159 \pmod{641}$，$2^{25}\equiv -636 = 5 \pmod{641}$，

$2^{32}\equiv 640\equiv -1 \pmod{641}$。

这就证明了所要结论。本题也可以通过计算 $2^8, 2^{16}, 2^{32}$对模641的剩余来算，这时数目要大些。

例 4　证明不定方程 $x^2+2y^2=203$ 无解。

由 $203=7\cdot 29$ 知，若有解 x_0, y_0，则必有 $(x_0y_0, 203)=1$。显见有 $x_0^2\equiv -2y_0^2 \pmod 7$。由于 $(y_0, 7)=1$，由性质Ⅷ知 y_0对模7有逆y_0^{-1}。在同余式两边乘 $(y_0^{-1})^2$得

$$(x_0y_0^{-1})^2\equiv x_0^2(y_0^{-1})^2\equiv -2y_0^2(y_0^{-1})^2$$
$$\equiv -2(y_0y_0^{-1})^2\equiv -2 \pmod 7.$$

但 n^2对模 7 的剩余仅可能是：$0, 1, -3, 2$，不可能是 -2，所以原方程无解。

例 5　设 $n\geqslant 1$，b 的素因数都大于n。证明：对任意正整数 a 必有

$$n! \mid a(a+b)(a+2b)\cdots(a+(n-1)b).$$

证　由条件知 $(b, n!)=1$。由性质Ⅷ知，b 对模 $n!$有逆 b^{-1}。我们有

$$(b^{-1})^n\cdot a(a+b)\cdots(a+(n-1)b)$$

$$\equiv ab^{-1}(ab^{-1}+bb^{-1})\cdots(ab^{-1}+(n-1)bb^{-1})$$
$$\equiv ab^{-1}(ab^{-1}+1)\cdots(ab^{-1}+(n-1))(\bmod n!).$$

上式右端是 n 个相邻整数乘积，因此，由第一章§8推论4得到

$$(b^{-1})^n\cdot a(a+b)\cdots(a+(n-1)b)\equiv 0(\bmod n!).$$

由于 $(b^{-1},n!)=1$，由此从性质Ⅵ就推出

$$a(a+b)\cdots(a+(n-1)b)\equiv 0(\bmod n!).$$

这就证明了所要的结论。

例6 设 $m>n\geqslant 1$。求最小的 $m+n$ 使得

$$1000\mid 1978^m-1978^n.$$

问题就是要求最小的 $m+n$ 使

$$1978^m-1978^n\equiv 0(\bmod 1000) \tag{9}$$

成立。先来讨论使上式成立的 m,n 要满足什么条件。记 $k=m-n$。式(9)即

$$2^n\cdot 989^n(1978^k-1)\equiv 0(\bmod 2^3\cdot 5^3).$$

由性质Ⅶ，Ⅸ知，它等价于

$$\begin{cases}2^n\equiv 0(\bmod 2^3), & (10)\\ 1978^k-1\equiv 0(\bmod 5^3). & (11)\end{cases}$$

由(10)知 $n\geqslant 3$。下面来求使(11)成立的 k。先求使

$$1978^l-1\equiv 0(\bmod 5)$$

成立的最小的 l，记作 d_1。由于

$$1978\equiv 3(\bmod 5).$$

所以 $d_1=4$。再求使

$$1978^h-1\equiv 0(\bmod 5^2)$$

成立的最小的 h，记作 d_2。由第一章§4例7知 $4\mid d_2$，注意到

$$1978\equiv 3(\bmod 5^2),$$

由例2的计算知，$d_2=20$。最后求使

$$1978^k-1\equiv 0(\bmod 5^3)$$

成立的最小的 k，记作 d_3。由第一章§4例7知 $20\mid d_3$。注意到

$$1978\equiv -22(\bmod 5^3),$$

$$(-22)^{20}\equiv(25-3)^{20}\equiv 3^{20}\equiv(243)^4$$
$$\equiv 7^4\equiv(50-1)^2\equiv 26 \pmod{5^3}.$$

通过计算得

$$1978^{20}\equiv 26 \pmod{5^3},\qquad 1978^{40}\equiv(25+1)^2\equiv 51 \pmod{5^3},$$
$$1978^{60}\equiv(25+1)(50+1)\equiv 76 \pmod{5^3},$$
$$1978^{80}\equiv(50+1)^2\equiv 101 \pmod{5^3},$$
$$1978^{100}\equiv(100+1)(25+1)\equiv 1 \pmod{5^3}.$$

因此，$d_3=100$。所以由第一章§4例7知必有$100|k$，最小的$k=100$。由此推出为使式(10)和(11)，即式(9)成立的充要条件是

$$n\geqslant 3,\qquad 100|m-n.$$

所以，最小的$m+n=(m-n)+2n=106$。

习 题 一

1. 分别求出$a=359$，1378对模$m=4,8,13,43$的最小非负剩余、最小正剩余、及绝对最小剩余。

2. 对哪些模m以下各同余式成立：(i) $32\equiv 11 \pmod m$；(ii) $1000\equiv -1 \pmod m$；(iii) $2^8\equiv 1 \pmod m$。

3. 对哪些模m，同余式$32\equiv 11 \pmod m$及$1000\equiv -1 \pmod m$同时成立。一般地，使同余式$a\equiv b \pmod m$及$c\equiv d \pmod m$同时成立的模m要满足什么条件？

4. (i) 素数$p>2$对模$m=4$的最小非负剩余、最小正剩余、及绝对最小剩余可能取哪些值？

(ii) (i)中改为$p>3$，$m=6$；

(iii) (i)中改为$p>5$，$m=30$。

具体举出素数p分别取到(i),(ii),(iii)中所说的剩余。

5. 证明：(i) $a\equiv b \pmod m$等价于$a-b\equiv 0 \pmod m$；

(ii) 若$a\equiv b \pmod m$，$c\equiv d \pmod m$，则$a-c\equiv b-d \pmod m$。

从同余式的运算角度来解释这两个结果的意义。

6. 利用同余式符号及其性质来证明或求解第一章§3习题

三的第 5,6,7,8,9,16,29,30,31 题。

7. 判断以下结论是否成立。对的给以证明，错的举出反例.

(i) 若 $a^2\equiv b^2 \pmod m$ 成立，则 $a\equiv b \pmod m$。

(ii) 若 $a^2\equiv b^2 \pmod m$，则 $a\equiv b \pmod m$ 或 $a\equiv -b \pmod m$ 至少有一个成立。

(iii) 若 $a\equiv b \pmod m$，则 $a^2\equiv b^2 \pmod {m^2}$。

(iv) 若 $a\equiv b \pmod 2$，则 $a^2\equiv b^2 \pmod {2^2}$。

(v) 设 p 是奇素数，$p\nmid a$。那么，$a^2\equiv b^2 \pmod p$ 成立的充要条件是 $a\equiv b \pmod p$ 或 $a\equiv -b \pmod p$ 有且仅有一式成立。

(vi) 设 $(a,m)=1$，$k\geqslant 1$.那么，从 $a^k\equiv b^k \pmod m$，$a^{k+1}\equiv b^{k+1} \pmod m$ 同时成立可推出 $a\equiv b \pmod m$。

8. 当正整数 m 满足什么条件时，

$$1+2+\cdots+(m-1)+m\equiv 0 \pmod m$$

一定成立（不要计算左边的和式）。

9. 当正整数 m 满足什么条件时，

$$1^3+2^3+\cdots+(m-1)^3+m^3\equiv 0 \pmod m$$

一定成立（不要计算左边的和式）。

10. 对任意正整数 $n\geqslant 1$，$1+2+\cdots+n$ 表为十进制数时，它的最后一位数可能取哪些值？

11. 设素数 $p\nmid a$，$k\geqslant 1$。证明：$n^2\equiv an \pmod {p^k}$ 成立的充要条件是 $n\equiv 0 \pmod {p^k}$ 或 $n\equiv a \pmod {p^k}$。

12. 设 $n>4$。证明：n 是合数的充要条件是

$$(n-2)!\equiv 0 \pmod n).$$

13. 证明：$70!\equiv 61! \pmod {71}$。

14. (i) 求 2^{400} 对模10的最小非负剩余；(ii) 求 2^{1000} 的十进位表示中的最后两位数字；(iii) 求 9^{9^9} 及 $9^{9^{9^9}}$ 的十进位表示中的最后两位数字；(iv) 求 $(13481^{56}-77)^{28}$ 被111除后所得的最小非负余数；(v) 求 2^s 对模10的最小非负剩余，$s=2^k$，$k\geqslant 2$。

15. (i) 求 3 对模 7 的逆；(ii) 求13对模10的逆。

16. 设 a^{-1} 是 a 对模 m 的逆. 证明:

(i) $an\equiv c\pmod m$ 成立的充要条件是 $n\equiv a^{-1}c\pmod m$;

(ii) $a^{-1}b^{-1}$ 是 ab 对模 m 的逆, 即 $(ab)^{-1}\equiv a^{-1}b^{-1}\pmod m$. 特别对任意正整数 k, $(a^k)^{-1}\equiv(a^{-1})^k\pmod m$.

17. 求整数 n 满足 (i) $3n\equiv 5\pmod 7$; (ii) $13n\equiv 7\pmod{10}$.

18. 求整数 n 同时满足 $n\equiv 1\pmod 4$, $n\equiv 2\pmod 3$.

19. 证明: 对任意整数 n, 下面五个同余式中至少有一个成立: $n\equiv 0\pmod 2$, $n\equiv 0\pmod 3$, $n\equiv 1\pmod 4$, $n\equiv 5\pmod 6$, $n\equiv 7\pmod{12}$.

20. 证明: 对任意整数 n, 下面六个同余式中至少有一个成立:

$$n\equiv 0\pmod 2,\quad n\equiv 0\pmod 3,\quad n\equiv 1\pmod 4,$$

$$n\equiv 3\pmod 8,\quad n\equiv 7\pmod{12},\quad n\equiv 23\pmod{24}.$$

21. 证明以下不定方程无解: (i) $x^2-2y^2=77$; (ii) $x^2-3y^2+5z^2=0$.

22. 求出所有的正整数三元组 $\{a,b,c\}$, 满足条件:

$$a\equiv b\pmod c,\quad b\equiv c\pmod a,\quad c\equiv a\pmod b.$$

23. 求出所有的非零整数三元组 $\{a,b,c\}$, 满足条件:

$$a\equiv b\pmod{|c|},\quad b\equiv c\pmod{|a|},\quad c\equiv a\pmod{|b|}.$$

24. 设 p 是素数, $f(x)$ 是整系数多项式,

$$f(x)=q(x)(x^p-x)+r(x),$$

$q(x)$ 及 $r(x)$ 是整系数多项式, $r(x)$ 的次数 $<p$. 证明: 对所有整数 x,

$$f(x)\equiv r(x)\pmod p,$$

即这是一个模 p 的恒等同余式.

25. 设 p 是素数, $f(x)$ 是整系数多项式. 再设 $a_1,\cdots,a_k$ 两两对模 p 不同余, 满足 $f(a_j)\equiv 0\pmod p$, $1\leqslant j\leqslant k$. 证明: 存在整系数多项式 $q(x)$, 使得

$$f(x)\equiv q(x)(x-a_1)\cdots(x-a_k)\pmod p,$$

这里的符号同 § 1式(5)。进而证明：

$$x^{p-1}-1\equiv(x-1)\cdots(x-p+1)\pmod p, \tag{a}$$

$$x^{p}-x\equiv x(x-1)\cdots(x-p+1)\pmod p, \tag{b}$$

$$(p-1)!\equiv-1\pmod p, \tag{c}$$

以及 $p>3$时，

$$\sum_{1\leqslant i<j\leqslant p-1} ij\equiv 0\pmod p. \tag{d}$$

26. 设素数 $p>3$。证明：

$$\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\cdots+\frac{(p-1)!}{(p-1)}\equiv 0\pmod{p^2}.$$

§ 2　同余类与剩余系

定义1　同余类（剩余类）　由 § 1 性质 I 知，对给定的模 m，整数的同余关系是一个等价关系，因此全体整数可按对模 m 是否同余分为若干个两两不相交的集合，使得在同一个集合中的任意两个数对模 m 一定同余，而属于不同集合中的两个数对模 m 一定不同余。每一个这样的集合称为是模 m 的同余类，或模 m 的剩余类。我们以 $r \bmod m$ 表 r 所属的模 m 的同余类。

由定义立即推出

定理1　(i) $r \bmod m=\{r+km:\ k\in\mathbf{Z}\}$；

(ii) $r \bmod m=s \bmod m$ 的充要条件是 $r\equiv s\pmod m$；

(iii) 对任意的 r,s，要么 $r \bmod m=s \bmod m$，要么 $r \bmod m$ 与 $s \bmod m$ 的交集为空集。

定理 I (ii) 表明同余式就是同余类（看作为一个元素）的等式，因此，§1 中关于同余式的性质都可表述为同余类的性质。这些将安排在习题中。

定理2　对给定的模 m，有且恰有 m 个不同的模 m 的同余类，

它们是

$$0 \bmod m, 1 \bmod m, \cdots, (m-1) \bmod m. \quad (1)$$

证 由定理1(ii)知这是m个两两不同的同余类。对每个整数a，由第一章§3定理1知

$$a = qm + r, \quad 0 \leqslant r < m.$$

因此，由定理1(i)知，$a \in r \bmod m$，即a必属于(1)中的某个同余类。证毕。

由定理2及鸽巢原理立即推出：

定理3 (i) 在任意取定的$m+1$个整数中，必有两个数对模m同余；

(ii) 存在m个数两两对模m不同余。

证 因为对模m共有m个由式(1)给出的同余类，所以$m+1$个数中必有两个数属于同一个模m的同余类，这两个数就对模m同余。这就证明了(i)。在每个同余类$r \bmod m (0 \leqslant r < m)$中取定一个数$x_r$作代表，这样就得到$m$个两两对模$m$不同余的数$x_0$，$x_1, \cdots, x_{m-1}$。这就证明了(ii)。

由定理3可引进以下概念：

定义2(完全剩余系) 一组数$y_1, \cdots, y_s$称为是**模m的完全剩余系**，如果对任意的a有且仅有一个y_j是a对模m的剩余，即a同余于y_j模m。

由定义中y_j的唯一性知这s个数一定是两两对模m不同余。由定理3知，模m的完全剩余系是存在的，且$s=m$，以及给定的m个数是一组模m的完全剩余系的充要条件是它们两两对模m不同余。事实上，一组模m的完全剩余系就是在模m的每个同余类中取定一个数作为代表所构成的一组数；而对于一组模m的完全剩余系$y_1, \cdots, y_m$，

$$y_1 \bmod m, \cdots, y_m \bmod m \quad (2)$$

就是模m的m个两两不同的同余类，以及

$$Z = \bigcup_{1 \leqslant j \leqslant m} y_j \bmod m. \tag{3}$$

容易直接验证：$0,\cdots,m-1$；$1,\cdots,m$；$-[m/2],\cdots,-[-m/2]-1$（当m是偶数时也可取为$-[m/2]+1,\cdots,-[-m/2]$）；$-m+1,\cdots,0$；$-m,\cdots,-1$等都是模m的完全剩余系，它们分别称为**模 m 的最小非负（完全）剩余系；最小正（完全）剩余系；绝对最小（完全）剩余系；最大非正（完全）剩余系；最大负（完全）剩余系**。由式(1)知，对任意取定的m个整数$k_r(0\leqslant r<m)$，

$$r+k_r m, \quad 0\leqslant r<m \tag{4}$$

是模m的一组完全剩余系，以及对模m的任给的一组完全剩余系，一定可以选取适当的$k_r(0\leqslant r<m)$，使它由式(4)表出。一般地，由式(2)知，当$y_j(1\leqslant j\leqslant m)$是任给的一组模$m$的完全剩余系时，对任取的整数$h_j(1\leqslant j\leqslant m)$，

$$y_j+h_j m, \quad 1\leqslant j\leqslant m, \tag{4'}$$

是模m的一组完全剩余系；反过来，对模m的任意一组完全剩余系，一定可以选取适当的$h_j(1\leqslant j\leqslant m)$，使它由式(4)表出。例如：取$k_r=0(0\leqslant r<m)$，式(4)就给出了模$m$的最小非负剩余系；取$k_0=m, k_r=0(1\leqslant r<m)$，式(4)就给出了模$m$的最小正剩余系；取$k_r=0(0\leqslant r\leqslant m/2)$；$k_r=-1(m/2<r\leqslant m-1)$，式(4)就给出模$m$的绝对最小剩余系；取$k_r=-1(0\leqslant r<m)$，式(4)就给出了模$m$的最大负剩余系；以及取$k_0=0, k_r=-1(1\leqslant r<m)$，式(4)就给出模$m$的最大非正剩余系。再例如，取$y_j=j(1\leqslant j\leqslant m), h_j=j(1\leqslant j\leqslant m)$，则由式(4')得到模$m$的完全剩余系：$(m+1)\cdot 1, (m+1)\cdot 2,\cdots,(m+1)\cdot m$；取$y_j=-j(1\leqslant j\leqslant m), h_j=j(1\leqslant j\leqslant m)$，则由式(4')得到模$m$的完全剩余系：$(m-1)\cdot 1,(m-1)\cdot 2,\cdots,(m-1)\cdot m$；在式(4')中取$h_j=y_j a_j(1\leqslant j\leqslant m$，$a_j$为任意整数)，就得到模$m$的完全剩余系：

$$(a_1m+1)y_1,\cdots,(a_mm+1)y_m.$$

显见，任意两组模 m 的完全剩余系，它们各自元素之和对模 m 是同余的。容易求出：这和同余于

$$0+1+\cdots+(m-1)\equiv(m-1)m/2$$

$$\equiv\begin{cases}0\pmod m, & 2\nmid m,\\ m/2\pmod m, & 2\mid m.\end{cases} \tag{5}$$

定理4 设 $m_1\mid m$。那么，对任意的 r 有

$$r \bmod m\subseteq r \bmod m_1,$$

等号仅当 $m_1=m$ 时成立。更精确地说，若 $l_1,\cdots,l_d$ 是模 $d=m/m_1$ 的一组完全剩余系，则

$$r \bmod m_1=\bigcup_{1\leqslant j\leqslant d}(r+l_jm_1)\bmod m, \tag{6}$$

右边和式中的 d 个模 m 的同余类两两不同。特别地有

$$r \bmod m_1=\bigcup_{0\leqslant j<d}(r+jm_1)\bmod m. \tag{7}$$

证 只要证明式(6)。我们把同余类 $r \bmod m_1$ 中的数按模 m 来分类。对 $r \bmod m_1$ 中任意两个数 $r+k_1m_1,r+k_2m_1$,

$$r+k_1m_1\equiv r+k_2m_1\pmod m$$

成立的充要条件是（利用§1性质Ⅶ）：

$$k_1\equiv k_2\pmod d.$$

由此就推出式(6)右边和式中的 d 个模 m 的同余类是两两不同的，且 $r \bmod m_1$ 中的任一数 $r+km_1$ 必属于其中的一个同余类。另一方面，对任意的 j 必有

$$(r+l_jm_1)\bmod m\subseteq(r+l_jm_1)\bmod m_1=r \bmod m_1.$$

这就证明了所要的结论。

在定理4中取 $m_1=1,r=0$，式(6)就是式(3)，因此定理4是式(3)的推广。应该指出，第一章§3例1—例3中讨论的集合

$S_{a,j}$ 就是同余类 $j \bmod a$。例1就是定理2，而例3则是给出了定理4的具体例子：$m_1=2$，$m=6$，$r=1$，$l_j=j-1(1\leqslant j\leqslant 3)$。定理4是经常用到的，通常是用以下同余式语言的表述。

定理4′ 设 $m_1|m$。那么，对任意的 r，

$$n\equiv r(\bmod m_1)$$

成立的充要条件是以下 $d=m/m_1$ 个同余式有且仅有一个成立：

$$n\equiv r+jm_1(\bmod m),\quad 0\leqslant j<d.$$

例如，取 $m_1=2$，奇数 $n\equiv 1(\bmod 2)$，若取 $m=4$，则 $n\equiv 1(\bmod 4)$，$n\equiv 3(\bmod 4)$ 有且必有一个成立；若取 $m=8$，则 $n\equiv 1,3,5$，或 $7(\bmod 8)$ 有且必有一个成立。取 $m_1=3$，对 $n\equiv -1(\bmod 3)$，若取 $m=6$，则 $n\equiv -1$ 或 $2(\bmod 6)$ 有且必有一个成立；若取 $m=15$，则 $n\equiv -1,2,5,8,11\ (\bmod 15)$ 有且必有一个成立。

在进一步讨论既约同余类、既约剩余系之前，先来给出第一章§4例10的另一种解法，以说明引进同余类的概念是有好处的。

例1 同第一章§4例10。

我们的想法是把要涂色的集合 M 扩充到全体整数，满足：(a) 属于同一个模 n 的同余类中的数涂相同的颜色；(b) 仍保持条件(i)，(ii)成立。这样，为使条件(ii)成立，必须满足：(iii) 0和 k 要涂同一种颜色。这样，我们就对全体整数 $\mathbf{Z}$ 涂色，满足条件(a)及(i)，(ii)，(iii)。我们来考察这样的涂色有什么性质。

(1) 对任意的 $j\in\mathbf{Z}$，j 和 $-j$ 一定涂相同的颜色。因为必有 $0\leqslant i<n$，使 $j\equiv i(\bmod n)$，由(a)知 j 和 i 同色。当 $i=0$ 时，$-j\equiv j\equiv 0(\bmod n)$，所以由(a)知 j 和 $-j$ 同色；当 $0<i<n$ 时，由(i)知 i 和 $n-i$ 同色，进而由(a)知 i 和 $-i$，$-i$ 和 $-j$ 同色，所以，亦有 j 和 $-j$ 同色。

(2) 对任意的 $j\in\mathbf{Z}$，j 和 $j\pm k$ 同色，即属于同一个模 k 的同余类中的数涂同色。因为必有 $0\leqslant i<n$ 使 $j\equiv i(\bmod n)$，由(a)

知 j 和 i 同色，由(ii)和(iii)知 i 和 $|k-i|$ 同色，进而由(1)推出 $|k-i|$ 和 $i-k$ 同色，而由(a)知 $i-k$ 和 $j-k$ 同色，所以 j 和 $j-k$ 同色。由此及(1)推得，j 和 $-j,-j-k$，$j+k$ 都同色。这就证明了所要结论。

由(a)和(2)知，任一 $j\in \mathbf{Z}$ 必和 $j+sn+tk$ 同色，这里 s,t 是任意整数。由 $(n,k)=1$，知必有 s_0,t_0 使得 $s_0n+t_0k=1$，所以，j 和 $j+1$ 同色。这就证明了所有整数都涂同一种颜色。

这一解法比第一章§4例10的解法要思路清晰、自然，且看出了这种涂色方法的实质是满足条件(a)和(2)。

为了引进既约同余类、既约剩余系的概念，先证明一个定理。

定理5 模 m 的一个同余类中的任意两个整数 a_1,a_2 与 m 的最大公约数相等，即 $(a_1,m)=(a_2,m)$。

证 设 $a_1\in r \bmod m$，$a_2\in r \bmod m$。由定理1(i)知 $a_j=r+k_jm$，$j=1,2$。进而由第一章§4定理1(iv)得

$$(a_j,m)=(r+k_jm,m)=(r,m),\quad j=1,2.$$

这就证明了所要的结论。

定义3 模 m 的同余类 $r \bmod m$ 称为是**模 m 的既约（或互素）同余类**，如果 $(r,m)=1$。模 m 的所有既约同余类的个数记作 $\phi(m)$，通常称为 Euler 函数。

定义4 一组数 $z_1,\cdots,z_t$ 称为是**模 m 的既约（或互素）剩余系**，如果 $(z_j,m)=1,1\leqslant j\leqslant t$；以及对任意的 $a,(a,m)=1$，有且仅有一个 z_j 是 a 对模 m 的剩余，即 a 同余于 z_j 模 m。

由定理5知，既约同余类的定义是合理的，即不会因为一个同余类中的代表元素 r 取得不同而得到矛盾的结论。由定义及定理2（以 $m \bmod m$ 代 $0 \bmod m$）立即推出

定理6 模 m 的所有不同的既约同余类是：

$$r \bmod m,\quad (r,m)=1,\quad 1\leqslant r\leqslant m. \tag{8}$$

$\phi(m)$ 等于 $1,2,\cdots,m$ 中和 m 既约的数的个数。

由于每个和 m 既约的数必属于某个模 m 的既约同余类，所以

由定理 6 及鸽巢原理立即推出（证明留给读者）

定理7 （i）在任意取定的 $\phi(m)+1$ 个均和 m 既约的整数中，必有两个数对模 m 同余；

（ii）存在 $\phi(m)$ 个数两两对模 m 不同余且均和 m 既约。

由定义 4 中 z_j 的唯一性知这 t 个数一定两两对模 m 不同余．由定理 7 知既约剩余系是存在的，且 $t=\phi(m)$。事实上，模 m 的既约剩余系就是在模 m 的每个既约同余类中取定一个数作代表所构成的一组数，因此它的一般形式是：

$$r+k_r m, \quad (r,m)=1, \quad 1\leqslant r\leqslant m, \tag{9}$$

其中 k_r 是任意取定的整数；而对于模 m 的一组既约剩余系 $z_1, \cdots, z_{\phi(m)}$，

$$z_1 \bmod m, \cdots, z_{\phi(m)} \bmod m, \tag{10}$$

就给出了模 m 的 $\phi(m)$ 个两两不同的既约同余类。

应该指出的是：模 m 的一组完全剩余系中所有和 m 既约的数组成模 m 的一组既约剩余系。这一点在考虑问题时是有用的。此外，任意给定的 $\phi(m)$ 个和 m 既约的数，只要它们两两对模 m 不同余就一定是模 m 的既约剩余系。Euler 函数 $\phi(m)$ 在数论中是十分重要的．如何求它的值是首先要解决的问题，下面来讨论最简单的情形．

$m=1$ 时，模 1 的同余类只有一个：$0 \bmod 1$，它是既约同余类，所以 $\phi(1)=1$。0 或任一整数就构成模 1 的既约剩余系．$m=2$ 时，模 2 的同余类有两个：$0 \bmod 2$，$1 \bmod 2$。只有 $1 \bmod 2$ 是既约同余类，所以 $\phi(2)=1$。1 或任一奇数就构成模 2 的既约剩余系。模 4 的既约同余类是：$1 \bmod 4$，$3 \bmod 4$，$\phi(4)=2$，1,3 是模 4 的一组既约剩余系。模12的既约同余类是：$1 \bmod 12$，$5 \bmod 12$，$7 \bmod 12$，$11 \bmod 12$，$\phi(12)=4$，1,5,7,11 是模12的一组既约剩余系。当 $m=p^k$，p 是素数时有下面的结论．

定理8 设 p 是素数，$k\geqslant 1$。那么，

$$\phi(p^k)=p^{k-1}(p-1), \tag{11}$$

以及模 p^k 的既约同余类是：

$$(a+bp)\bmod p^k,\quad 1\leqslant a\leqslant p-1,\quad 0\leqslant b\leqslant p^{k-1}-1. \qquad (12)$$

证 由定理6知，$\phi(p^k)$ 等于满足以下条件的 r 的个数：

$$1\leqslant r\leqslant p^k,\quad (r,p^k)=1.$$

由于 p 是素数，所以有

$$(r,p)=\begin{cases}1, & p\nmid r,\\ p, & p\mid r.\end{cases}$$

由此及第一章§4定理10知：$(r,p^k)=1$ 的充要条件是 $(r,p)=1$，即 $p\nmid r$。因此，$\phi(p^k)$ 就等于 $1,2,\cdots,p^k$ 中不能被 p 整除的数的个数。由于 $1,2,\cdots,p^k$ 中能被 p 整除的数有 p^{k-1} 个，所以，$\phi(p^k)=p^k-p^{k-1}$，这就是式(11)。由带余数除法知，任一 r：$1\leqslant r\leqslant p^k, p\nmid r$，可表为

$$r=bp+a,\quad 1\leqslant a\leqslant p-1,\quad 0\leqslant b\leqslant p^{k-1}-1.$$

反过来，对任意满足 $1\leqslant a\leqslant p-1, 0\leqslant b\leqslant p^{k-1}-1$ 的 a,b，相应的 $r=bp+a$ 必满足 $1\leqslant r\leqslant p^k, p\nmid r$。这就证明了式(12)。

例如：$m=3^3$ 时，$\phi(3^3)=3^3-3^2=18$，模 3^3 的既约同余类是：

$$(a+b\cdot 3)\bmod 3^3,\quad 1\leqslant a\leqslant 2,\quad 0\leqslant b\leqslant 8.$$

1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26 就是模 3^3 的一组既约剩余系。如果取绝对最小剩余，那么，±1，±2，±4，±5，±7，±8，±9，±10，±11，±13 就是模 3^3 的一组既约剩余系。如何求一般的 $\phi(m)$ 将在§3讨论。

习 题 二（Ⅰ）

1．(i) 写出剩余类 3 mod 17 中不超过 100 的正整数；

(ii) 写出剩余类 6 mod 15 中绝对值不超过 90 的整数。

2．(i) 写出模 9 的一个完全剩余系，它的每个数是奇数；

(ii) 写出模 9 的一个完全剩余系，它的每个数是偶数。

(iii) (i)或(ii)中的要求对模 10 的完全剩余系能实现吗？

(iv) 若 $2|m$，则模 m 的一组完全剩余系中一定一半是偶数，一半是奇数。

3. 利用具体定出 § 2式(4)($m=7$)中的 k_r 的方法，写出模 7 的一个完全剩余系，使得它的元素都属于(i) 剩余类 0 mod 3；(ii) 剩余类 1 mod 3；(iii) 剩余类 2 mod 3。

4. 设 $(a,m)=1$，s 为任意整数。利用 § 2 式(4)证明：一定存在模 m 的完全剩余系，它的元素全部属于剩余类 s mod a。

5. 证明：当 $m>2$ 时，$0^2,1^2,\cdots,(m-1)^2$ 一定不是模 m 的完全剩余系。

6. 设 $r_1,\cdots,r_m$；$r'_1,\cdots,r'_m$ 分别是模 m 的两组完全剩余系。证明：当 m 是偶数时，$r_1+r'_1,\cdots,r_m+r'_m$ 一定不是模 m 的完全剩余系。

7. 设有 m 个整数，它们都不属于剩余类 0 mod m。那么，其中必有两个数之差属于剩余类 0 mod m。

8. 在任意取定的对模 m 两两不同余的 $[m/2]+1$ 个数中，必有两数之差属于剩余类 1 mod m。如何推广本题？

9. (i) 把剩余类 1 mod 5 写成模15的剩余类之和；(ii) 把剩余类 6 mod 10 写成模 120 的剩余类之和；(iii) 把剩余类 6 mod 10 写成模 80 的剩余类之和。

10. (i) $n\equiv 1 \pmod 2$ 的充要条件是 n 对模 10 的绝对最小剩余为哪些数？

(ii) $n\equiv -1 \pmod 5$ 的充要条件是 n 对模 45 的最小正剩余为哪些数？

11. 设 $n>2$ 为给定的整数。试问：模 $2n-1$ 的一组完全剩余系最少要属于模 $n-2$ 的几个剩余类？一般地，$K>m\geq 1$，模 K 的一组完全剩余系最少要属于模 m 的几个剩余类？

12. 具体写出模 $m=16,17,18$ 的最小非负既约剩余系、绝对最小既约剩余系，并算出 $\phi(16)$，$\phi(17)$，$\phi(18)$。

13. 把第 3,4 题中的完全剩余系改为既约剩余系。

14. 设 $m\geqslant3$，$r_1,\cdots,r_s$ 是所有小于 $m/2$ 且和 m 既约的正整数。证明：$-r_s,\cdots,-r_1,r_1,\cdots,r_s$ 及 $r_1,\cdots,r_s,(m-r_s),\cdots,(m-r_1)$ 都是模 m 的既约剩余系。由此推出当 $m\geqslant3$ 时 $2|\phi(m)$。

15. 设 $m\geqslant3$。证明：

(i) 模 m 的一组既约剩余系的所有元素之和对模 m 必同余于零；

(ii) 模 m 的最小正既约剩余系的各数之和等于 $m\phi(m)/2$。这结论对 $m=2$ 也成立。

16. 以 $\tilde{0},\tilde{1},\cdots,\widetilde{m-1}$ 记模 m 的 m 个剩余类。在由这 m 个元素组成的集合 $\boldsymbol{Z}_m$ 中定义"加法"$\oplus$及"乘法"$\odot$如下：对任意的 $0\leqslant a,b\leqslant m-1$，

$$\tilde{a}\oplus\tilde{b}=\tilde{c},\quad 0\leqslant c\leqslant m-1,$$

只要 $c\equiv a+b(\bmod m)$；及

$$\tilde{a}\odot\tilde{b}=\tilde{c},\quad 0\leqslant c\leqslant m-1,$$

只要 $c\equiv ab(\bmod m)$。证明

(i) 这样定义的加法和乘法是一定可以实现的，且 $\tilde{c}$ 是唯一的；

(ii) 这样定义的加法和乘法满足交换律、结合律、以及分配律：即 $\tilde{a}\oplus\tilde{b}=\tilde{b}\oplus\tilde{a}$，$(\tilde{a}\oplus\tilde{b})\oplus\tilde{c}=\tilde{a}\oplus(\tilde{b}\oplus\tilde{c})$，及 $\tilde{a}\odot(\tilde{b}\oplus\tilde{c})=(\tilde{a}\odot\tilde{b})\oplus(\tilde{a}\odot\tilde{c})$；

(iii) $\tilde{0}$是$\boldsymbol{Z}_m$ 中的零元素，即对任意$\tilde{a}$，必有 $\tilde{a}\oplus\tilde{0}=\tilde{a}$，及$\tilde{a}\odot\tilde{0}=\tilde{0}$；

(iv) $\tilde{1}$ 是$\boldsymbol{Z}_m$ 中的乘法单位元素，即对任意的 $\tilde{a}$，必有 $\tilde{a}\odot\tilde{1}=\tilde{a}$（当 $m=1$ 时，仅有一个元素 $\tilde{0}$）。

(v) 对任意的两个元素 $\tilde{a},\tilde{b}$，必有唯一的一个元素 $\tilde{x}$ 满足 $\tilde{b}+\tilde{x}=\tilde{a}$，$\tilde{x}$ 就称为 $\tilde{a}$ 与 $\tilde{b}$ 之差，记作$\tilde{x}=\tilde{a}\ominus\tilde{b}$。特别的，当 $\tilde{a}=\tilde{0}$，记 $-\tilde{b}=\tilde{0}\ominus\tilde{b}$，证明：当$\tilde{b}=\tilde{0}$时，$-\tilde{b}=\tilde{0}$，当$\tilde{b}\neq\tilde{0}$，时 $-\tilde{b}=(\widetilde{m-b})$；

(vi) 当 $m\geqslant2$，$(a,m)=1$ 时，必有 $\tilde{x}$ 满足 $\tilde{a}\odot\tilde{x}=\tilde{1}$，$\tilde{x}$ 是唯一的。$\tilde{x}$ 称为是元素 $\tilde{a}$ 的逆，记作 $\tilde{a}^{-1}$。进而证明：$(\tilde{a}^{-1})^{-1}=\tilde{a}$，

$(\bar{a}\odot\bar{b})^{-1}=\bar{a}^{-1}\odot\bar{b}^{-1}$。

(vii) 设 $m\geqslant 2$，$(a,m)=1$。那么，对任意的 $\bar{b}$；必有唯一的 $\bar{x}$ 满足 $\bar{a}\odot\bar{x}=\bar{b}$，以及 $\bar{x}=(\bar{a}^{-1})\odot\bar{b}$；

(viii) 举例说明：对任意的 $\bar{a},\bar{b}$，不一定有 $\bar{x}$ 满足 $\bar{a}\odot\bar{x}=\bar{b}$，即 $\bar{a}$ 不一定能"整除" $\bar{b}$，即不一定能作"除法"；

(ix) 证明：当 p 是素数时，$\bar{1},\cdots,\widetilde{(p-1)}$ 中的任意两个元素都可作除法；

(x) 在满足 $(a,m)=1$ 的全体 $\phi(m)$ 个元素 $\bar{a}$ 中，任意两个元素都可作"除法"。下面列表说明当 $m=10$ 时这样定义的运算(见表 1 和表 2)，并请读者自己逐项验证或举例说明题中的结论。

表1　Z_{10} 中的加法表

$\oplus$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$
$\tilde{0}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$
$\tilde{1}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$
$\tilde{2}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$
$\tilde{3}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{4}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$
$\tilde{5}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$
$\tilde{6}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{7}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$
$\tilde{8}$	$\tilde{8}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$
$\tilde{9}$	$\tilde{9}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$

17．列出 Z_{13}，Z_{14} 中的加法表与乘法表。

18．设 $d\geqslant 1, d\mid n$。证明：$n-\phi(n)\geqslant d-\phi(d)$，等号仅当 $d=n$ 时成立。

19．证明：存在无穷多个正整数 n，使得 $\phi(n)>\phi(n+1)$。此外，举例说明存在正整数 n 使得(i) $\phi(n)=\phi(n+1)$；(ii) $\phi(n)$

表2　Z_{10} 中的乘法表

$\odot$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$
$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$
$\tilde{1}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$	$\tilde{6}$	$\tilde{7}$	$\tilde{8}$	$\tilde{9}$
$\tilde{2}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$	$\tilde{6}$	$\tilde{8}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$	$\tilde{6}$	$\tilde{8}$
$\tilde{3}$	$\tilde{0}$	$\tilde{3}$	$\tilde{6}$	$\tilde{5}$	$\tilde{2}$	$\tilde{5}$	$\tilde{8}$	$\tilde{1}$	$\tilde{4}$	$\tilde{7}$
$\tilde{4}$	$\tilde{0}$	$\tilde{4}$	$\tilde{8}$	$\tilde{2}$	$\tilde{6}$	$\tilde{0}$	$\tilde{4}$	$\tilde{8}$	$\tilde{2}$	$\tilde{6}$
$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{0}$	$\tilde{5}$
$\tilde{6}$	$\tilde{0}$	$\tilde{6}$	$\tilde{2}$	$\tilde{8}$	$\tilde{4}$	$\tilde{0}$	$\tilde{6}$	$\tilde{2}$	$\tilde{8}$	$\tilde{4}$
$\tilde{7}$	$\tilde{0}$	$\tilde{7}$	$\tilde{4}$	$\tilde{1}$	$\tilde{8}$	$\tilde{5}$	$\tilde{2}$	$\tilde{9}$	$\tilde{6}$	$\tilde{3}$
$\tilde{8}$	$\tilde{0}$	$\tilde{8}$	$\tilde{6}$	$\tilde{4}$	$\tilde{2}$	$\tilde{0}$	$\tilde{8}$	$\tilde{6}$	$\tilde{4}$	$\tilde{2}$
$\tilde{9}$	$\tilde{0}$	$\tilde{9}$	$\tilde{8}$	$\tilde{7}$	$\tilde{6}$	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$	$\tilde{2}$	$\tilde{1}$

$=\phi(n+2)$；(iii) $\phi(n)=\phi(n+3)$。

20．设 p_1,p_2 是两个不同的素数，证明：在 $1,2,\cdots,p_1p_2$ 中，被 p_1 整除的数的个数等于 p_2；被 p_2 整除的数的个数等于 p_1；被 p_1p_2 整除的数有 1 个，由此推出

$$\phi(p_1p_2)=(p_1-1)(p_2-1)=\phi(p_1)\cdot\phi(p_2)。$$

21．设 n,h 是正整数．证明：在不超过 nh 的正整数中，和 n 既约的数的个数等于 $h\phi(n)$。

22．利用第20题的方法，证明：

(i) 设 p_1,p_2,p_3 是三个不同的素数，则

$$\phi(p_1p_2p_3)=(p_1-1)(p_2-1)(p_3-1)；$$

(ii) 设 $p_1,\cdots,p_k$ 是 k 个不同的素数，则

$$\phi(p_1\cdots p_k)=(p_1-1)\cdots(p_k-1)。$$

23．利用第21题来证明上题的结论。

24．设 m 的素因数分解式是 $p_1^{\alpha_1}\cdots p_r^{\alpha_r}$．证明：

$$\phi(m)=p_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1}\phi(p_1\cdots p_r)$$

$$=p_1^{\alpha_1-1}(p_1-1)\cdots p_r^{\alpha_r-1}(p_r-1)$$

$$=\phi(p_1^{\alpha_1})\cdots\phi(p_r^{\alpha_r}).$$

现在来讨论剩余系的整体性质及其结构。

定理9 (i) 设 c 是任意整数。那么，x 遍历模 m 的一组完全剩余系时，$x+c$ 也遍历模 m 的一组完全剩余系。也就是说，$x_1,\cdots,x_m$ 是模 m 的一组完全剩余系的充要条件是 $x_1+c,\cdots,x_m+c$ 是模 m 的一组完全剩余系。

(ii) 设 $k_1,\cdots,k_{\phi(m)}$ 是任意整数。那么，$y_1,\cdots,y_{\phi(m)}$ 是模 m 的一组既约剩余系的充要条件是 $y_1+k_1m,\cdots,y_{\phi(m)}+k_{\phi(m)}m$ 是模 m 的一组既约剩余系。

证明是显然的，留给读者。

定理10 设 $(a,m)=1$。那么，x 遍历模 m 的完全（既约）剩余系的充要条件是 ax 遍历模 m 的完全（既约）剩余系。也就是说，$x_1,\cdots,x_s$ 是模 m 的完全（既约）剩余系的充要条件是 $ax_1,\cdots,ax_s$ 是模 m 的完全（既约）剩余系。

证 由§1性质VII知：当 $(a,m)=1$ 时，对任意的 i,j 有

$$x_i\not\equiv x_j\pmod m\Longleftrightarrow ax_i\not\equiv ax_j\pmod m,\qquad(13)$$

以及由第一章§4定理10知：当 $(a,m)=1$ 时，对任意的 i 有

$$(ax_i,m)=(x_i,m).\qquad(14)$$

对于完全剩余系来说，定理中的 $s=m$，由此及式(13)就推出关于完全剩余系的结论，因为 m 个数只要两两对模 m 不同余就一定是模 m 的完全剩余系。对于既约剩余系来说，$s=\phi(m)$，由此及式(13)，(14)就推出关于既约剩余系的结论，因为 $\phi(m)$ 个均和 m 既约的数，只要两两对模 m 不同余就一定是模 m 的既约剩余系。

定理10表明：只要 $(a,m)=1$，我们就可以找到这样的模 m 的完全剩余系和既约剩余系，它们的元素都是 a 的倍数；而当 $(a,m)>1$ 时，这是一定不可能的。例如 $3\cdot0,3\cdot1,\cdots,3\cdot7$ 是模 8

的完全剩余系，$3\cdot1,3\cdot3,3\cdot5,3\cdot7$ 是模 8 的既约剩余系。取 $a=-1$ 就推出 x 与 $-x$ 同时遍历模 m 的完全(既约)剩余系。结合定理 9,10 及式(4)就可得到各种形式的完全或既约剩余系。

定理11 设 $m=m_1m_2$, $x_i^{(1)}(1\leqslant i\leqslant m_1)$ 是模 m_1 的完全剩余系，$x_j^{(2)}(1\leqslant j\leqslant m_2)$ 是模 m_2 的完全剩余系。那么，$x_{ij}=x_i^{(1)}+m_1x_j^{(2)}$ 是模 m 的完全剩余系．也就是说当 $x^{(1)},x^{(2)}$ 分别遍历模 m_1，模 m_2 的完全剩余系时，$x=x^{(1)}+m_1x^{(2)}$ 遍历模 $m=m_1m_2$ 的完全剩余系。

证 这定理实际上是定理 4 的直接推论。我们下面给一个直接证明。这时 x_{ij} 共有 $m=m_1m_2$ 个数，因此只要证明它们两两对模 m 不同余。若

$$x_{i_1}^{(1)}+m_1x_{j_1}^{(2)}\equiv x_{i_1j_1}\equiv x_{i_2j_2}\equiv x_{i_2}^{(1)}+m_1x_{j_2}^{(2)}(\bmod m_1m_2), \tag{15}$$

则必有

$$x_{i_1}^{(1)}\equiv x_{i_2}^{(1)}(\bmod m_1),$$

由此及 $x_i^{(1)}$ 在同一个模 m 的完全剩余系中取值，所以必有 $x_{i_1}^{(1)}=x_{i_2}^{(1)}$，$i_1=i_2$。由此及式(15)得

$$m_1x_{j_1}^{(2)}\equiv m_1x_{j_2}^{(2)}(\bmod m_1m_2),$$

即

$$x_{j_1}^{(2)}\equiv x_{j_2}^{(2)}(\bmod m_2),$$

因而同理有 $x_{j_1}^{(2)}=x_{j_2}^{(2)}$，$j_1=j_2$。这就证明了所要的结论。

定理11刻画了完全剩余系的某种结构，表明大模 $m=m_1m_2$ 的完全剩余系，可以某种形式表为两个较小的模 m_1、模 m_2 的完全剩余系的组合。利用归纳法可把定理11推广为

定理12 设 $m=m_1m_2\cdots m_k$，及

$$x=x^{(1)}+m_1x^{(2)}+m_1m_2x^{(3)}+\cdots+m_1\cdots m_{k-1}x^{(k)}, \tag{16}$$

那么，当 $x^{(j)}(1\leqslant j\leqslant k)$ 分别遍历模 m_j 的完全剩余系时，x 遍历模 m 的完全剩余系。也就是说，当 $x_{i_j}^{(j)}(1\leqslant i_j\leqslant m_j)$ 是模 m_j

的完全剩余系（$1\leqslant j\leqslant k$）时，

$$x_{i_1 i_2\cdots i_k}=x_{i_1}^{(1)}+m_1x_{i_2}^{(2)}+m_1m_2x_{i_3}^{(3)}+\cdots+m_1\cdots m_{k-1}x_{i_k}^{(k)},$$

$$1\leqslant i_j\leqslant m_j,\quad 1\leqslant j\leqslant k$$

是模 m 的完全剩余系。

证　由定理11知结论对 $k=2$ 成立。假设结论对 $k=n(\geqslant 2)$ 成立，当 $k=n+1$ 时，设 $\overline{m}_n=m_1\cdots m_n$，以及

$$\bar{x}^{(n)}=x^{(1)}+m_1x^{(2)}+\cdots+m_1\cdots m_{n-1}x^{(n)},$$

则有

$$x=\bar{x}^{(n)}+\overline{m}_nx^{(n+1)}.$$

由归纳假设知，当 $x^{(j)}(1\leqslant j\leqslant n)$ 遍历模 m_j 的完全剩余系时，$\bar{x}^{(n)}$ 遍历模 $\overline{m}_n$ 的完全剩余系。而由上式及结论对 $k=2$ 成立知，$\bar{x}^{(n)}, x^{(n+1)}$ 分别遍历模 $\overline{m}_n$，模 m_{n+1} 的完全剩余系时，x 就遍历模 $\overline{m}_n\overline{m}_{n+1}=m_1\cdots m_{n+1}$ 的完全剩余系，即结论对 $k=n+1$ 成立。证毕。

定理11与定理12的优点是对模 m_j 不加限制条件，但一般说来对既约剩余系没有相应结果成立（请读者举例说明）。但在以下特殊情形下，可对既约剩余系得到一个有用结果。我们说两个整数 a 和 b 有相同的素因数，是指素数 $p|a$ 的充要条件是 $p|b$。如果定理12中的 m_1 与 m 有相同素因数，即若素数 $p|m$，则必有 $p|m_1$（注意这里 $m_1|m$），那么，

$$(x,m)=1\Longleftrightarrow(x^{(1)},m_1)=1,$$

这里 x 由式(16)给出。由于一个完全剩余系中所有与模既约的数构成一个既约剩余系，所以从以上讨论就证明了

定理13　在定理12的条件与符号下，设 m_1 和 m 有相同的素因数。那么，当 $x^{(1)}$ 遍历模 m_1 的完全（既约）剩余系，$x^{(j)}(2\leqslant j\leqslant k)$ 分别遍历模 m_j 的完全剩余系时，x 遍历模 m 的完全（既约）剩余系。特别地，当 $m_1=m_2=\cdots=m_k=n$ 时，当 $x^{(1)}$ 遍历模 n 的完全（既约）剩余系，$x^{(j)}(2\leqslant j\leqslant k)$ 分别遍历模 n 的完全剩余系时，

$$x = x^{(1)} + nx^{(2)} + n^2x^{(3)} + \cdots + n^{k-1}x^{(k)} \qquad (17)$$

遍历模 n^k 的完全(既约)剩余系。

容易看出，定理13的后一部分结论实际上就是用整数的 n 进位表示来构造模 n^k 的完全(既约) 剩余系， 当 $n=$ 素数 p 时这就是定理 8 . 把定理10和11相结合，当$(m_1,m_2)=1$时，由于 $x^{(1)}$和 $m_2x^{(1)}$同时遍历模 m_1 的完全剩余系，所以，这时从定理 11 立即推出：若设

$$x = m_2x^{(1)} + m_1x^{(2)}, \qquad (18)$$

那么，当 $x^{(j)}(j=1,2)$遍历模 m_j 的完全剩余系时， 由式(18)给出的 x 也遍历模 $m=m_1m_2$ 的完全剩余系。 在式(18)中 m_1,m_2 处于对称形式(而这一点之所以可能是因为$(m_1,m_2)=1$)，这比原来的不对称形式显然要方便。事实上，不仅如此，在这条件下可证明更强的结论，在作进一步讨论之前，先举两个例子来说明定理13。

例 2 利用模10，模199的完全剩余系来表示模1990的完全剩余系。

解 (i) $x=x^{(1)}+10x^{(2)}$，当$x^{(1)}$遍历模10的完全剩余系及当$x^{(2)}$遍历模199的完全剩余系时，x 遍历模1990的完全剩余系。特别地，取 $1\leqslant x^{(1)}\leqslant 10$，$0\leqslant x^{(2)}\leqslant 198$ 时， x 取值 $1,2,\cdots,1990$；取$0\leqslant x^{(1)}\leqslant 9$，$0\leqslant x^{(2)}\leqslant 198$ 时， x 取$0,1,\cdots,1989$；取 $-4\leqslant x^{(1)}\leqslant 5$，$-99\leqslant x^{(2)}\leqslant 99$时， x 取值 $-994,-993,\cdots,995$，即取模1990的绝对最小完全剩余系。

(ii) $x=x^{(1)}+199x^{(2)}$，当 $x^{(1)}$，$x^{(2)}$分别遍历模199，模10的完全剩余系时， x 遍历模1990的完全剩余系。特别地，取$1\leqslant x^{(1)}\leqslant 199$，$0\leqslant x^{(2)}\leqslant 9$时， x 取值 $1,2,\cdots,1990$； 取 $0\leqslant x^{(1)}\leqslant 198$，$0\leqslant x^{(2)}\leqslant 9$时， x 取$0,1,\cdots,1989$；取 $-198\leqslant x^{(1)}\leqslant 0$， $-4\leqslant x^{(2)}\leqslant 5$时， x 取值 $-994,-993,\cdots,995$，即是模 1990 的绝对最小完全剩余系；取 $1\leqslant x^{(1)}\leqslant 199$， $-5\leqslant x^{(2)}\leqslant 4$时， x 也取值 $-994,-993,\cdots,995$。

(iii) $x=199x^{(1)}+10x^{(2)}$. 由于$(199,10)=1$，从定理10知$x^{(1)}$和$199x^{(1)}$同时遍历模10的完全剩余系，所以当$x^{(1)},x^{(2)}$分别遍历模10，模199的完全剩余系时，x遍历模1990的完全剩余系。此外，由下面的定理14知，当$x^{(1)},x^{(2)}$分别遍历模10，模199的既约剩余系时，x也遍历模1990的既约剩余系。

例 3 利用模3的剩余系来表示模$3^n(n\geqslant 2)$的剩余系。

解 由定理13知，当$x^{(1)}$遍历模3的完全(既约)剩余系，$x^{(j)}(2\leqslant j\leqslant n)$遍历模3的完全剩余系时，

$$x=x^{(1)}+3x^{(2)}+\cdots+3^{n-1}x^{(n)}$$

遍历模3^n的完全(既约)剩余系。特别的，取$x^{(1)}=0,1,2$(或$1,2$)，$x^{(j)}=0,1,2(2\leqslant j\leqslant n)$时，$x$遍历模$3^n$的最小非负完全(或既约)剩余系；取$x^{(1)}=1,2,3$(或$1,2$)，$x^{(j)}=0,1,2(2\leqslant j\leqslant n)$时，$x$遍历模$3^n$的最小正完全(或既约)剩余系；取$x^{(1)}=-1,0,1$(或$-1,1$)，$x^{(j)}=-1,0,1(2\leqslant j\leqslant n)$时，$x$遍历模$3^n$的绝对最小完全（或既约）剩余系。

利用上面所说的绝对最小完全剩余系的表示法，可得出一个有趣的应用：利用n个重量分别为1克，3克，3^2克，$\cdots$，3^{n-1}克的砝码，可以在天平上秤出重量在1克到$(3^n-1)/2$克之间的物体的重量(误差不超过1克)。请读者自己说明这一应用的道理。

定理14 设$m=m_1m_2$，$(m_1,m_2)=1$，x由式(18)给出。那么，x遍历模m的完全(既约)剩余系的充要条件是$x^{(1)},x^{(2)}$同时分别遍历模m_1,m_2的完全(既约)剩余系。也就是说，若

$$x_{ij}=m_2x_i^{(1)}+m_1x_j^{(2)}\quad(1\leqslant i\leqslant s,1\leqslant j\leqslant t),$$

那么，$x_{ij}(1\leqslant i\leqslant s,1\leqslant j\leqslant t)$是模$m$的完全(既约)剩余系的充要条件是：$x_i^{(1)}(1\leqslant i\leqslant s)$是模$m_1$的完全(既约)剩余系，以及$x_j^{(2)}(1\leqslant j\leqslant t)$是模$m_2$的完全(既约)剩余系。

证 先对完全剩余系来证。先证充分性。这时$s=m_1,t=m_2$。所以x_{ij}共有m_1m_2个数。对任意的$1\leqslant i_1,i_2\leqslant m_1$，$1\leqslant j_1,j_2\leqslant m_2$，由条件$(m_1,m_2)=1$及§1性质Ⅸ知，

$$x_{i_1j_1}\equiv x_{i_2j_2}\pmod m$$

等价于

$$x_{i_1j_1}\equiv x_{i_2j_2}\pmod{m_1},\quad x_{i_1j_1}\equiv x_{i_2j_2}\pmod{m_2},$$

即等价于

$$m_2x_{i_1}^{(1)}\equiv m_2x_{i_2}^{(1)}\pmod{m_1},\qquad m_1x_{j_1}^{(2)}\equiv m_1x_{j_2}^{(2)}\pmod{m_2}.$$

由§1性质Ⅵ及$(m_1,m_2)=1$知，这等价于

$$x_{i_1}^{(1)}\equiv x_{i_2}^{(1)}\pmod{m_1},\qquad x_{j_1}^{(2)}\equiv x_{j_2}^{(2)}\pmod{m_2}.$$

由于$x_i^{(1)},x_j^{(2)}$分别在同一个模m_1,m_2的完全剩余系中取值，所以必有$i_1=i_2,j_1=j_2$。这就证明了这m_1m_2个x_{ij}两两对模m不同余，即是模m的一组完全剩余系。

下证必要性。由$x_{ij}(1\leqslant i\leqslant s,1\leqslant j\leqslant t)$是模$m$的完全剩余系，所以，$st=m=m_1m_2$。取定$x_1^{(2)}$，由

$$x_{i1}=m_2x_i^{(1)}+m_1x_1^{(2)},\qquad 1\leqslant i\leqslant s$$

对模$m=m_1m_2$两两不同余，所以$m_2x_i^{(1)}$也对模m_1m_2两两不同余，即

$$m_2x_{i_1}^{(1)}\not\equiv m_2x_{i_2}^{(1)}\pmod{m_1m_2},\qquad 1\leqslant i_1\neq i_2\leqslant s.$$

这等价于

$$x_{i_1}^{(1)}\not\equiv x_{i_2}^{(1)}\pmod{m_1},$$

即这s个$x_i^{(1)}$对模m_1两两不同余，所以$s\leqslant m_1$。同理可证t个$x_j^{(2)}$对模m_2两两不同余，所以$t\leqslant m_2$。由此及$st=m_1m_2$推出$s=m_1$，$t=m_2$，这就证明了必要性。

为了证明对既约剩余系的结论，我们只要证明(为什么)：

$$(x,m_1m_2)=1$$

成立的充要条件是

$$(x^{(1)},m_1)=(x^{(2)},m_2)=1. \tag{19}$$

由于$(x,m_1m_2)=1$等价于

$$(m_2x^{(1)}+m_1x^{(2)},m_1)=(m_2x^{(1)}+m_1x^{(2)},m_2)=1,$$

这就是

$$(m_2x^{(1)},m_1)=(m_1x^{(2)},m_2)=1.$$

由于$(m_1,m_2)=1$，由第一章§4定理10知，上式等价于式(19)。证毕

由定理14利用归纳法，如同证明定理12一样，立即推出：

定理15 设 $m=m_1\cdots m_k$，$m_1,\cdots,m_k$ 两两既约。再设 $m=m_jM_j(1\leqslant j\leqslant k)$，及

$$x=M_1x^{(1)}+\cdots+M_kx^{(k)}. \tag{20}$$

那么，x 遍历模 m 的完全(既约)剩余系的充要条件是 $x^{(1)},\cdots,x^{(k)}$分别遍历模 $m_1,\cdots,m_k$ 的完全(既约)剩余系。

证 $k=2$ 即定理14，所以成立。设$k=n(\geqslant 2)$定理成立。当$k=n+1$ 时，$m=m_1\cdots m_nm_{n+1}$。设 x 由式(20)$(k=n+1)$给出，

$$\bar{x}^{(n)}=\frac{m}{m_1m_{n+1}}x^{(1)}+\cdots+\frac{m}{m_nm_{n+1}}x^{(n)}.$$

我们有

$$x=m_{n+1}\bar{x}^{(n)}+\frac{m}{m_{n+1}}x^{(n+1)}.$$

由以上两式，从归纳假设及定理对 $k=2$ 成立，就推出所要结论。

由定理15及定理10就推出(证明留给读者)：

定理16 在定理15的符号和条件下，再设 $a_j(1\leqslant j\leqslant k)$是任意取定的整数，满足$(a_j,m_j)=1\ (1\leqslant j\leqslant k)$。那么，

$$x=a_1M_1x^{(1)}+\cdots+a_kM_kx^{(k)} \tag{21}$$

遍历模 m 的完全(既约)剩余系的充要条件是 $x^{(j)}(1\leqslant j\leqslant k)$分别遍历模 m_j 的完全(既约)剩余系。

定理15与定理16是等价的(为什么)。定理14,15,16是十分重要的，它们实际上就是关于一次同余方程组的孙子定理(见第四

章§3定理1、定理2)。比较定理11和定理14可以看出，定理11只是证明了：$x^{(1)},x^{(2)}$分别遍历模 m_1，模 m_2 的完全剩余系是$x=x^{(1)}+m_1x^{(2)}$遍历模 m_1m_2的完全剩余系的充分条件。容易看出，这条件不是必要的，例如：

例 4 取$m_1=2,m_2=4,m=m_1m_2=8$。再取 $x_1^{(1)}=1,x_2^{(1)}=2,x_3^{(1)}=5,x_4^{(1)}=6$；$x_1^{(2)}=0,x_2^{(2)}=1$。这样$x_i^{(1)}+2x_j^{(2)}(1\leqslant i\leqslant 4,1\leqslant j\leqslant 2)$就取值1,2,5,6,3,4,7,8是模 8 的完全剩余系。

例 5 取 $m_1=3,m_2=4,m=m_1m_2=12$。再取 $x_i^{(1)}=i$，$1\leqslant i\leqslant 6$；$x_1^{(2)}=0,x_2^{(2)}=2$。不难算出$x_i^{(1)}+3x_j^{(2)}(1\leqslant i\leqslant 6,1\leqslant j\leqslant 2)$是模12的一组完全剩余系。

下面我们举例说明定理14,15,16中的剩余系形式的特点。

例 6 以模30为例具体给出形如式(20)，(21)的完全剩余系和既约剩余系。

解 (i) 在式(20)中 取 $k=2$(即式(18))，$m_1=6$，$m_2=5$。这时 $M_1=5$，$M_2=6$，

$$x=5x^{(1)}+6x^{(2)}. \tag{22}$$

取模 6 的完全剩余系 $x^{(1)}$：

$$-2,\underline{-1},0,\underline{1},2,3, \tag{23}$$

这样，$5x^{(1)}$也遍历模 6 的完全剩余系，取值为

$$-10,\underline{-5},0,\underline{5},10,15; \tag{24}$$

取模 5 的完全剩余系$x^{(2)}$：

$$\underline{-2},\underline{-1},0,\underline{1},\underline{2}, \tag{25}$$

这样，$6x^{(2)}$也遍历模 5 的完全剩余系，取值为

$$\underline{-12},\underline{-6},0,\underline{6},\underline{12}.$$

因此，由式(22)给出的模 30 的完全剩余系可由下面的加法表（见表 3）给出：

表 3

$6x^{(2)}$ \ $5x^{(1)}$ +	-10	-5	0	5	10	15
-12	-22	-17	-12	-7	-2	3
-6	-16	-11	-6	-1	4	9
0	-10	-5	0	5	10	15
6	-4	1	6	11	16	21
12	2	7	12	17	22	27

以上各式和表 3 中的相应的既约剩余系由数字下面画一虚线表出。

如果在式(21)中取 $k=2$。仍取 $m_1=6$，$m_2=5$。取 a_1, a_2满足 $a_1M_1\equiv1 \pmod{m_1}$，$a_2M_2\equiv1 \pmod{m_2}$，即

$$5a_1\equiv1 \pmod 6,\qquad 6a_2\equiv1 \pmod 5.$$

所以，可取 $a_1=-1$，$a_2=1$。这样，式(21)变为

$$x=-5x^{(1)}+6x^{(2)}. \tag{26}$$

当 $x^{(1)}, x^{(2)}$仍分别取由式(23)，(25)给出的模 6，模 5 的完全剩余系时，由式(26)给出的模 30 的完全剩余系由下面的加法表（见表 4）给出。表中相应的既约剩余系由数字下面画一虚线表出。

(ii) 在式(20)中取 $k=3, m_1=2, m_2=3, m_3=5$.这时$M_1=15$，$M_2=10, M_3=6$，

$$x=15x^{(1)}+10x^{(2)}+6x^{(3)}. \tag{27}$$

取 $x^{(1)}$ 遍历模 2 的完全剩余系：

$$0, 1, \tag{28}$$

表 4

$-5x^{(1)}$ / $6x^{(2)}$ / +	10	5	0	−5	−10	−15
−12	−2	−7	−12	−17	−22	−27
−6	4	1	−6	−11	−16	−21
0	10	5	0	−5	−10	−15
6	16	11	6	1	−4	−9
12	22	17	12	7	2	−3

这样，$15x^{(1)}$遍历模 2 的完全剩余系：

$$0, 15; \tag{29}$$

取$x^{(2)}$遍历模 3 的完全剩余系：

$$-1, 0, 1, \tag{30}$$

这样，$10x^{(2)}$遍历模 3 的完全剩余系：

$$-10, 0, 10; \tag{31}$$

取$x^{(3)}$遍历模 5 的完全剩余系：

$$-2, -1, 0, 1, 2, \tag{32}$$

这样，$6x^{(3)}$遍历模 5 的完全剩余系：

$$-12, -6, 0, 6, 12. \tag{33}$$

因此，由式(27)给出的模30的完全剩余系可由下面的加法表（见表 5）给出。以上各式和表中相应的既约剩余系由数字下面画一虚线表出。

如果在式(21)中取 $k=3$，仍取 $m_1=2$，$m_2=3$，$m_3=5$，那

表 5

$15x^{(1)}$ / $10x^{(2)}$ (+)	0	15										
−10	−10	5	−22	−7	−16	−1	−10	5	−4	11	2	17
0	0	15	−12	3	−6	9	0	15	6	21	12	27
10	10	25	−2	13	4	19	10	25	16	31	22	37
	$15x^{(1)}+10x^{(2)}$ (+) / $6x^{(3)}$		−12		−6		0		6		12	

么，取 $a_1=a_2=a_3=1$，就满足 $a_jM_j\equiv 1(\bmod m_j)(1\leqslant j\leqslant 3)$。所以，这时给出的模30的完全(既约)剩余系和上面讨论的相同。

读者可能会觉得这样来求剩余系既麻烦，所得的形式又似乎很不规律。那么究竟有什么好处呢？为了说明这一点，我们来指出由式(20),(21)给出的剩余系的特点。以下的符号及满足的条件和定理15,16相同。

(1) 对任一 l $(1\leqslant l\leqslant k)$，$y^{(l)}=M_lx^{(l)}$(或 $a_lM_lx^{(l)}$)与 $x^{(l)}$ 同时是模 m_l 的完全(既约)剩余系。模 m_l 的这一形式的剩余系具有这样的特点：它的每个元素被任一 $m_j(j\neq l)$ 整除，即

$$y^{(l)}\equiv 0\ (\bmod m_j),\qquad j\neq l. \tag{34}$$

(2) 模 $m_1,\cdots$，模 m_k 的这种特殊形式的完全(既约)剩余系 $y^{(1)},\cdots,y^{(k)}$ 的"和" $y^{(1)}+\cdots+y^{(k)}=x$ 就给出了模 $m=m_1\cdots m_k$ 的完全(既约)剩余系，这一点对任意选取的模 m_l $(1\leqslant l\leqslant k)$ 的剩余系不一定成立。例如，模 2 的完全(既约)剩余系取$\{0,1\}$，模 3 的完全(既约)剩余系取$\{-1,0,1\}$，那么，直接作这样的"和"(即不乘以M_l或a_lM_l)得到数集合$\{-1,0,1,0,1,2\}$，它们

不是模 6 的完全(既约)剩余系①.

(3) 由式(20)或(21)给出的模 m 的完全(既约)剩余系 x 对模 m_l 的剩余仅和 $x^{(l)}$ 有关，与 $x^{(j)}(j\neq l)$ 的取值无关，即

$$x\equiv M_l x^{(l)}(\text{或 } a_l M_l x^{(l)})(\bmod m_l),\quad 1\leqslant l\leqslant k. \tag{35}$$

特别地，若所取的 a_l 满足

$$a_l M_l\equiv 1 \pmod{m_l}, \tag{36}$$

则由式(21)给出的 x 总有

$$x\equiv x^{(l)} \pmod{m_l}. \tag{37}$$

(4) 对固定的 l，在式(20)或(21)中命每个 $x^{(j)}(j\neq l)$ 取指定的值 b_j(b_j 的值可随 $x^{(l)}$ 取不同的值而取不同的指定的值)．这样，当 $x^{(l)}$ 遍历模 m_l 的完全(既约)剩余系时，由式(20)或(21)给出的 x 也遍历模 m_l 的完全(既约)剩余系，且 x 对模 m_j $(j\neq l)$的剩余为 $M_j b_j$ 或 $a_j M_j b_j$.

以上各点可通过例 6 中的三个表来一一验证．因此，利用式(20),(21)，灵活选取 m_l 及 a_l，就可得到模 m、模 m_l 的满足各种条件的剩余系，这在数论中是十分重要的．下面再举两个例子．

例 7 求模13的一组完全剩余系 $r_1,\cdots,r_{13}$，满足

$$r_i\equiv i(\bmod 3),\quad r_i\equiv 0(\bmod 7),\quad 1\leqslant i\leqslant 13.$$

解 在式(21)中取 $k=3$，$m_1=13$，$m_2=3$，$m_3=7$．这样，$M_1=21$，$M_2=91$，$M_3=39$．再取 $a_2=a_3=1$，及 a_1 为任一和 m_1 既约的数．这样，由(4)知(下面取 i' 为 i 对模 3 的绝对最小剩余)：当 $x_i^{(1)}(1\leqslant i\leqslant 13)$是模13的完全剩余系时，

$$r_i=21a_1x_i^{(1)}+91i'+39\cdot 0,\quad 1\leqslant i\leqslant 13,$$

就是我们所要的模13的完全剩余系．若取 $x_i^{(1)}(1\leqslant i\leqslant 13)$依次为

① 既约剩余系及运算所得的数，以数下面加虚线表示．

$$-6,-5,-4,\cdots,-1,0,1,\cdots,4,5,6,$$

当取 $a_1=1$ 时得到 $r_i(1\leqslant i\leqslant 13)$ 依次为：

$$r_1=21\cdot(-6)+91\cdot 1=-35,$$
$$r_2=21\cdot(-5)+91\cdot(-1)=-196,$$
$$r_3=21\cdot(-4)+91\cdot 0=-84,$$
$$r_4=21\cdot(-3)+91\cdot 1=28,$$
$$r_5=21\cdot(-2)+91\cdot(-1)=133,$$
$$r_6=21\cdot(-1)+91\cdot 0=-21,$$
$$r_7=21\cdot 0+91\cdot 1=91,$$
$$r_8=21\cdot 1+91\cdot(-1)=-70,$$
$$r_9=21\cdot 2+91\cdot 0=42,$$
$$r_{10}=21\cdot 3+91\cdot 1=154,$$
$$r_{11}=21\cdot 4+91\cdot(-1)=-7,$$
$$r_{12}=21\cdot 5+91\cdot 0=105,$$
$$r_{13}=21\cdot 6+91\cdot 1=217.$$

当取 $a_1=5$ 时， $a_1M_1=5\cdot 21\equiv 1(\mathrm{mod}\ 13)$， 这时必有 $r_i\equiv x_i^{(1)}(\mathrm{mod}\ 13)(1\leqslant i\leqslant 13)$，所取值依次为：

$$-539,-616,-420,-224,-35,-105,91,$$
$$14,210,406,329,525,721.$$

从以上所得的结果，容易得到具有所说性质的模13的既约剩余系。

例 8　设 m 的素因数分解式为 $p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，求指数和

$$S=\sum_{x\bmod m}{}' e^{2\pi i x/m} \tag{38}$$

的值，这里求和号 $\sum\limits_{x\bmod m}{}'$ 表示对模 m 的任意一组既约剩余系求和。

由于对任意整数 a， $e^{2\pi i a}=1$，所以指数和(38)的值与既约剩余系的具体选取无关。以 $\sum\limits_{x\bmod m}$ 表对模 m 的一组完全剩余系求

和，对任意整数 c 我们有

$$\sum_{x \bmod m} e^{2\pi i c x/m} = \sum_{x=1}^{m} e^{2\pi i c x/m}$$

$$= \begin{cases} m, & m \mid c, \\ 0, & m \nmid c. \end{cases} \tag{39}$$

由定理15知，若取 $m_j = p_j^{\alpha_j} (1 \leqslant j \leqslant r)$，$m_j M_j = m$，则当 $x^{(j)}$ 分别遍历模 $p_j^{\alpha_j}$ 的既约剩余系时，

$$x = M_1 x^{(1)} + \cdots + M_r x^{(r)}$$

遍历模 m 的既约剩余系。因此，

$$S = \sum_{x^{(1)} \bmod m_1}{}' \cdots \sum_{x^{(r)} \bmod m_r}{}' e^{2\pi i (M_1 x^{(1)} + \cdots + M_r x^{(r)})/m}$$

$$= S_1 S_2 \cdots S_r,$$

其中

$$S_j = \sum_{x^{(j)} \bmod m_j}{}' e^{2\pi i x^{(j)}/m_j}, \quad 1 \leqslant j \leqslant r.$$

容易看出

$$S_j = \sum_{x^{(j)}=1}^{p_j^{\alpha_j}} \exp\left\{\frac{2\pi i x^{(j)}}{p_j^{\alpha_j}}\right\} - \sum_{y^{(j)}=1}^{p_j^{\alpha_j - 1}} \exp\left\{\frac{2\pi i y^{(j)}}{p_j^{\alpha_j - 1}}\right\}.$$

由此及式(39)推出

$$S_j = \begin{cases} -1, & \alpha_j = 1, \\ 0, & \alpha_j > 1. \end{cases}$$

因而得

$$S = \begin{cases} (-1)^r, & \alpha_1 = \cdots = \alpha_r = 1, \\ 0, & \text{其它}. \end{cases} \tag{40}$$

习 题 二（II）

1．详细写出利用定理 4 推出定理11的证明。

2. 试用定理12来做第一章习题三的第18题。

3. 设$m>1$，$(a,m)=1$。证明：

(i) 对任意整数 b， $\sum_{x \bmod m}\left\{\frac{ax+b}{m}\right\}=\frac{1}{2}(m-1)$；

(ii) $\sum_{x \bmod m}{}'\left\{\frac{ax}{m}\right\}=\frac{1}{2}\phi(m)$。

4. 具体写出模23的一组完全剩余系，使得它的每个元素(i) 都是 7 的倍数；(ii) 都是对模 7 同余于2。(iii) 都是对模 7 同余于 2 且对模 5 也同余于 2。

5. 具体写出模23的一组完全剩余系$r_1,\cdots,r_{23}$满足以下两个条件：$r_j\equiv 0 \pmod 7$，$r_j\equiv j \pmod 5$，$1\leqslant j\leqslant 23$。

6. 把第 4 题改为既约剩余系来做。

7. 试求模 4 的一组完全剩余系$r_1,\cdots,r_4$，模 5 的一组完全剩余系$s_1,\cdots,s_5$，使得(i) $r_is_j(1\leqslant i\leqslant 4,\ 1\leqslant j\leqslant 5)$是模20的完全剩余系；(ii) $r_i+s_j(1\leqslant i\leqslant 4,\ 1\leqslant j\leqslant 5)$及$r_is_j(1\leqslant i\leqslant 4,\ 1\leqslant j\leqslant 5)$同时是模20的完全剩余系。

8. 上题的两个结论对既约剩余系能成立吗？

9. 试求模 3 的一组完全剩余系 r，模 7 的一组完全剩余系 s，使得当 r 遍历模 3 的这组完全剩余系（或其中的既约剩余系），s 遍历模 7 的这组完全剩余系(或其中的既约剩余系)时，rs 遍历模21的完全(或既约)剩余系。

10. 设$m_1,\cdots,m_k$两两既约，$(a_j,m_j)=1$。证明：当$x^{(j)}$分别遍历模m_j的完全(既约)剩余系($1\leqslant j\leqslant k$)时，

$$x=(M_1a_1x^{(1)}+M_2+\cdots+M_k)(M_1+M_2a_2x^{(2)}+M_3+\cdots+M_k)\cdots(M_1+\cdots+M_{k-1}+M_ka_kx^{(k)})$$

遍历模$m=m_1\cdots m_k$的完全(既约)剩余系，这里$m_jM_j=m$，($1\leqslant j\leqslant k$)。此外，还满足

$$x\equiv a_jM_j^kx^{(j)} \pmod{m_j},\qquad 1\leqslant j\leqslant k.$$

解释本题的含意。

§3 $\phi(m)$的性质与Fermat-Euler定理

从上节证明的有关既约剩余系的性质就可得到计算$\phi(m)$的公式，它的重要性质，包括著名的Fermat-Euler定理。

定理1 设$m=m_1m_2$。(i) 若m_1与m有相同的素因数，那么，

$$\phi(m)=m_2\phi(m_1). \tag{1}$$

特别地，若$m>1$，

$$m=p_1^{\alpha_1}\cdots p_r^{\alpha_r},\qquad \alpha_j\geqslant 1, \tag{2}$$

则

$$\phi(m)=p_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1}\phi(p_1\cdots p_r). \tag{3}$$

(ii) 若$(m_1,m_2)=1$，则

$$\phi(m)=\phi(m_1)\phi(m_2). \tag{4}$$

特别地，若m由式(2)给出，则

$$\phi(m)=p_1^{\alpha_1-1}(p_1-1)\cdots p_r^{\alpha_r-1}(p_r-1)$$

$$=m\prod_{p\mid m}\left(1-\frac{1}{p}\right). \tag{5}$$

证 在§2定理13中取$k=2$即得式(1)，因为按定义，模m的既约剩余系的元素个数为$\phi(m)$，模m_1的既约剩余系元素个数为$\phi(m_1)$，而模m_2的完全剩余系元素个数为m_2。在式(1)中取$m_1=p_1\cdots p_r$即得式(3)。由§2定理14对既约剩余系的结论即得式(4)，因为按定义模m,m_1,m_2的既约剩余系的元素个数分别为$\phi(m)$，$\phi(m_1),\phi(m_2)$。由式(4)立即推出若$m=m_1m_2\cdots m_r$，$m_1,\cdots,m_r$两两既约，则

$$\phi(m)=\phi(m_1)\phi(m_2\cdots m_r)$$

$$=\phi(m_1)\phi(m_2)\cdots\phi(m_r). \tag{6}$$

当m由式(2)给出时，取$m_j=p_j^{\alpha_j}(1\leqslant j\leqslant r)$，利用§2定理8从

上式即得式(5)。

由式(5)知，除了$\phi(1)=\phi(2)=1$，必有

$$2\mid\phi(m),\quad m\geqslant 3. \tag{7}$$

定理2 对任意正整数m有

$$\sum_{d\mid m}\phi(d)=m.$$

我们对定理给出两个证明。第一个证明是利用第一章§6式(21)，及刚证明的式(4)。第二个证明是以分析完全剩余系和既约剩余系的关系推出。

证明一 当$m=1$时结论显然成立。当$m>1$时，设m有表示式(2)，则由第一章§6式(21)得

$$\sum_{d\mid m}\phi(d)=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}\phi(p_1^{e_1}\cdots p_r^{e_r}).$$

利用式(6)即得

$$\sum_{d\mid m}\phi(d)=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}\phi(p_1^{e_1})\cdots\phi(p_r^{e_r})$$

$$=\left(\sum_{e_1=0}^{\alpha_1}\phi(p_1^{e_1})\right)\cdots\left(\sum_{e_r=0}^{\alpha_r}\phi(p_r^{e_r})\right),$$

由§2定理8知

$$\sum_{e_j=0}^{\alpha_j}\phi(p_j^{e_j})=\phi(1)+\phi(p_j)+\cdots+\phi(p_j^{\alpha_j})$$

$$=1+(p_j-1)+(p_j^2-p_j)+\cdots+(p_j^{\alpha_j}-p_j^{\alpha_j-1})$$

$$=p_j^{\alpha_j}.$$

由以上两式就推出所要结论。

证明二 我们来把正整数

$$1,2,\cdots,j,\cdots,m \tag{8}$$

按其和m的最大公约数分类，即和m的最大公约数相同的作为一

类。这样，在m的正除数d和这样的正整数类之间建立了一个一一对应关系，即对于每个m的正除数d对应于集合(8)中所有和m的最大公约数为d的那些正整数组成的子集。显见，m的不同的正除数对应于不相交的子集合，所以，集合(8)就是所有这种子集之并集。我们来求这种子集：

$$(j,m)=d, \quad 1\leqslant j\leqslant m. \tag{9}$$

设$j=dh$，式(9)就等价于(利用第一章§4定理8)

$$(h,m/d)=1, \quad 1\leqslant h\leqslant m/d. \tag{10}$$

而由§2定理6知这样的h的个数为$\phi(m/d)$，这也就是满足式(9)的j的个数。因而由以上讨论知

$$m=\sum_{d\mid m}\phi\left(\frac{m}{d}\right), \tag{11}$$

由此及第一章§2定理2即得所要结论。证毕。

应该指出的是在证明二中实际上只用到了$\phi(m)$的定义而没有用$\phi(m)$的其它性质。但这里用到了初等数论中一个极其重要的论证方法：把一个整数集合(在这里是由式(8)给出)按其与对一个给定的正整数K(在这里是m)的最大公约数来分类。此外，由式(9)确定的j组成的子集，通过关系式$j=dh$由式(10)就可看出，它实际上是模m/d的既约剩余系乘以同一个d而得到，因此，实质上就是把模m完全剩余系分解成了模m/d的既约剩余系，d取模m的全体正除数。例如取$m=12$，正除数$d=1,2,3,4,6$。这种分解见表1。

模m的既约剩余系可以取种种不同的形式，但每个既约剩余系中所有数的乘积对模m是不变的，即若$r_1,\cdots,r_{\phi(m)}$；$r'_1,\cdots,r'_{\phi(m)}$都是模m的既约剩余系，那么，必有

$$\prod_{j=1}^{\phi(m)} r_j\equiv\prod_{j=1}^{\phi(m)} r'_j \pmod m. \tag{12}$$

由此及§2定理10就可推出著名的**Fermat-Euler**定理。

表 1

$(12,j)$ \ j	1	2	3	4	5	6	7	8	9	10	11	12
1	1				5		7				11	
2		2								10		
3			3						9			
4				4				8				
6						6						12

定理3 设$(a,m)=1$，则有

$$a^{\phi(m)}\equiv 1(\bmod m). \tag{13}$$

特别当p为素数时，对任意的a有

$$a^p\equiv a(\bmod p). \tag{14}$$

证 取$r_1,\cdots,r_{\phi(m)}$是模m的一组既约剩余系，由§2定理10知，当$(a,m)=1$时，$ar_1,\cdots,ar_{\phi(m)}$也是模m的既约剩余系。因此由式(12)得

$$\prod_{j=1}^{\phi(m)} r_j\equiv\prod_{j=1}^{\phi(m)}(ar_j)=a^{\phi(m)}\prod_{j=1}^{\phi(m)} r_j\ (\bmod m),$$

由于$(r_j,m)=1$，利用§1性质Ⅷ，从上式即得式(13)。当$m=p$为素数时，由式(13)及$\phi(p)=p-1$得

$$a^{p-1}\equiv 1(\bmod p),\quad p\nmid a. \tag{15}$$

由此推出对任意的a式(14)成立。证毕。

在式(13)中取$a=-1$，得$(-1)^{\phi(m)}-1\equiv 0(\bmod m)$，由此推出：当$m\geqslant 3$时必有$2\mid\phi(m)$。这给出了式(7)的一个更简单的证明。定理3给出了a对模m的逆a^{-1}的一个很方便的形式，即当$(a,m)=1$时，

$$a^{-1}\equiv a^{\phi(m)-1}\ (\bmod m). \tag{16}$$

通常把式(14)称为Fermat小定理，而式(13)称为Euler定

理．显然后者是前者的推广．事实上，Fermat小定理已在第一章§4例3中证明了，这里不仅给出了一个更简单的证明，而且揭示了这一定理的实质．还应该指出，Euler定理证明了比第一章§4例7更深刻的结论，即使得

$$a^d \equiv 1 \pmod{m} \tag{17}$$

成立的最小正整数 d，设为 d_0，必有 $d_0 \mid \phi(m)$．

以上围绕定理3的讨论自然会引出两个问题：(1)模 m 的既约剩余系的乘积对模 m 究竟同余于什么？这将在下节讨论．(2)在什么情形下，会有使(17)成立的最小正整数 $d_0 = \phi(m)$．这问题比较复杂，将在第五章讨论．但我们先可证明以下结论，由此也可看出这问题的重要性．

定理4 设 $(a,m)=1$．那么，d_0 是使式(17)成立的最小正整数 d 的充要条件是：

$$a^{d_0} \equiv 1 \pmod{m}, \tag{18}$$

及

$$a^0 = 1, a, \cdots, a^{d_0 - 1} \tag{19}$$

对模 m 两两不同余．特别地，$d_0 = \phi(m)$ 的充要条件是式(19)$(d_0 = \phi(m))$ 给出了模 m 的一组既约剩余系．

证 先证定理的第一部分．若 d_0 是使(17)成立的最小正整数 d，则式(18)当然成立．如果有 $0 \leqslant i < j < d_0$ 使得

$$a^j \equiv a^i \pmod{m},$$

则由§1性质Ⅶ得

$$a^{j-i} \equiv 1 \pmod{m}.$$

但 $1 \leqslant j-i < d_0$，这和 d_0 的最小性矛盾，因此由式(19)给出的 d_0 个数两两对模 m 不同余，这就证明了必要性．再证充分性，由式(19)给出的数两两对模 m 不同余推出，

$$a^j \not\equiv a^0 \equiv 1 \pmod{m}, \quad 1 \leqslant j < d_0,$$

由此及式(18)成立推出 d_0 是使(17)成立的最小正整数 d．

下面证定理的第二部分．先证明必要性．上面的必要性证明中已指出：由式(19)给出的$\phi(m)$个数两两对模m不同余，而由$(a,m)=1$知，它们均和m既约，所以这是一组模m的既约剩余系．充分性的证明由Euler定理

$$a^{\phi(m)}\equiv 1(\mathrm{mod}\ m)$$

(即式(18)成立)及上面的充分性证明推出．证毕．

当$d_0=\phi(m)$时，定理4给出了既约剩余系的一个极为方便的形式，这一点是十分重要的．

例1 设$m=2^l(l\geqslant 3)$，$a=5$．求使式(17)成立的最小正整数$d=d_0$．

解 由$\phi(2^l)=2^{l-1}$及$d_0|\phi(2^l)$知，$d_0=2^k$，$0\leqslant k\leqslant l-1$．先证对任意的$a$，$2\nmid a$，必有

$$a^{2^{l-2}}\equiv 1(\mathrm{mod}\ 2^l). \tag{20}$$

对l用归纳法来证式(20)．设$a=2t+1$．当$l=3$时

$$a^2=4t(t+1)+1\equiv 1(\mathrm{mod}\ 2^3),$$

所以式(20)成立．假设式(20)对$l=n(\geqslant 3)$成立．当$l=n+1$时，由

$$a^{2^{n-1}}-1=(a^{2^{n-2}}-1)(a^{2^{n-2}}+1),$$

及归纳假设推出

$$a^{2^{n-1}}-1\equiv 0(\mathrm{mod}\ 2^{n+1}),$$

即式(20)对$l=n+1$成立．这就证明了式(20)对任意的$l\geqslant 3$都成立．因此，对任意的$a(2\nmid a)$，它所对应的$d_0=2^k$，必有$0\leqslant k\leqslant l-2$．下面来求$a=5$时所对应的$d_0$．由

$$5^{2^0}\equiv 5^1\not\equiv 1(\mathrm{mod}\ 2^3), \tag{21}$$

及式(20)($a=5$，$l=3$)就推出$l=3$时，$d_0=2^{3-2}=2$．由

$$5^{2^1}\equiv 25\not\equiv 1(\mathrm{mod}\ 2^4),$$

及式(20)($a=5$, $l=4$)就推出$l=4$时，$d_0=2^{4-2}=2^2$。我们来证明：对任意的$l\geqslant3$，必有

$$5^{2^{l-3}}\not\equiv1(\bmod 2^l)。\qquad(22)$$

对l用归纳法。当$l=3$时，由式(21)知式(22)成立。假设式(22)对$l=n(\geqslant3)$成立。由于，当$l\geqslant3$时必有

$$5^{2^{l-3}}\equiv1(\bmod 2^{l-1}),\qquad(23)$$

这当$l=3$时可直接验证，当$l>3$时这就是式(20)。由归纳假设及式(23)知，

$$5^{2^{n-3}}=1+s\cdot2^{n-1},\quad 2\nmid s。$$

因而有(注意$n\geqslant3$)

$$5^{2^{n-2}}=1+s(1+s\cdot2^{n-2})2^n,\quad 2\nmid s(1+s\cdot2^{n-2})。$$

这就证明了式(22)当$l=n+1$时也成立。所以，式(22)对$l\geqslant3$都成立。由此推出(为什么)

$$5^{2^j}\not\equiv1(\bmod 2^l),\quad 0\leqslant j\leqslant l-3。$$

由此及式(20)就推出，当$a=5$时对应的$d_0=2^{l-2}$。从定理4知：当$l\geqslant3$时，

$$5^0=1,5^1,5^2,5^3,\cdots,5^{2^{l-2}-1},\qquad(24)$$

这2^{l-2}个数对模2^l两两不同余。

式(20)表明，对模$2^l(l\geqslant3)$不可能有形如(19)的既约剩余系。另一方面，从式(24)给出的2^{l-2}个数两两对模2^l不同余，

$$1\equiv5^j\not\equiv-5^j\equiv-1(\bmod 2^2),\quad 0\leqslant j<2^{l-2}$$

及$\phi(2^l)=2^{l-1}$就推出：

定理5 对模$2^l(l\geqslant3)$，以下2^{l-1}个数给出了它的一组既约剩余系：

$$(-1)^{j_0}5^{j_1},\quad 0\leqslant j_0<2,\ 0\leqslant j_1<2^{l-2}。\qquad(25)$$

事实上，对任意的$2\nmid g_0$，$l\geqslant3$（$l=3$时，$g_0\neq8k-1$），若使同余式(17)（$a=g_0$，$m=2^l$）成立的最小的$d=2^{l-2}$，那末，以下2^{l-1}个数给出了模2^l的一组既约剩余系：

$$(-1)^{j_0}g_0^{j_1},\quad 0\leqslant j_0<2,\ 0\leqslant j_1<2^{l-2}.\tag{26}$$

习 题 三

1．证明：(i) 必有无穷多个正整数n，使得$3\nmid\phi(n)$；

(ii) 对任一正整数$d\geqslant3$，必有无穷多个正整数n，使得$d\nmid\phi(n)$。

2．对给定的正整数k，仅有有限多个n使得$\phi(n)=k$。

3．证明：(i) $\phi(mn)=(m,n)\phi([m,n])$；

(ii) $\phi(mn)\phi((m,n))=(m,n)\phi(m)\phi(n)$；

(iii) 当$(m,n)>1$时，则有$\phi(mn)>\phi(m)\phi(n)$。

4．求最小正整数k，使得$\phi(n)=k$无解；恰有两个解；恰有三个解；恰有四个解（一个没有解决的猜想是：不存在正整数k，使得$\phi(n)=k$恰有一个解）。

5．求$\phi(n)=24$的全部正整数n。

6．求满足下列方程的所有正整数n：(i) $\phi(n)=\phi(2n)$；(ii) $\phi(2n)=\phi(3n)$；(iii) $\phi(3n)=\phi(4n)$。

7．求$\phi(n)=2^6$的全部正整数n。

8．设$n>1$，$f(n)$表示不超过n且与n既约的所有正整数之和，证明：若$f(n)=f(m)$，则$m=n$。

9．设a,b是给定的正整数。证明：存在无穷多对自然数m，n，使得$a\phi(m)=b\phi(n)$。

10．设k是给定的正整数，证明：一定存在正整数n使得

$$\phi(n)=\phi(n+k).$$

11．证明：若$n>1$，$\phi(m)=\phi(mn)$，则必有$n=2$，$2\nmid m$。

12．证明：(i) $\phi(n)>\sqrt{n}/2$；(ii) 若n为合数，则

$$\phi(n)\leqslant n-\sqrt{n}.$$

13. 求出所有的正整数 n，使得$\phi(n)|n$。

14. 设 $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，$p_j$是不同的奇素数，$(a,m)=1$。再设$c=[c_0,\phi(p_1^{\alpha_1}),\cdots,\phi(p_r^{\alpha_r})]$，其中 $c_0=1$，当 $\alpha_0=0$；$c_0=2^{\alpha_0-1}$，当 $1\leqslant\alpha_0\leqslant2$；$c_0=2^{\alpha_0-2}$，当 $\alpha_0\geqslant3$。证明：

$$a^c\equiv1\pmod m.$$

15. 设 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，$p_j$是不同的素数，$c_j=\phi(p_j^{\alpha_j})$，$\alpha=\max(\alpha_1,\cdots,\alpha_r)$。证明：对任意整数 a 有

(i) $a^{\alpha+\phi(m)}\equiv a^\alpha\pmod m$； (ii) $a^m\equiv a^{m-\phi(m)}\pmod m$；

(iii) $a^\alpha f(a)\equiv0\pmod m$，其中$f(x)$是多项式$x^{c_1}-1,\cdots,x^{c_r}-1$的最小公倍式。解释本题的含意。

16. 设$(m,n)=1$。证明：$m^{\phi(n)}+n^{\phi(m)}\equiv1\pmod{mn}$。

17. 设 $f(x)$是整系数多项式.证明：$(f(x))^p\equiv f(x^p)\pmod p$，其中 p 是素数。

18. 设素数$p>2$，$a>1$。证明：

(i) a^p-1的素因数 q 必是$a-1$的因数，或是 $q\equiv1\pmod{2p}$；

(ii) a^p+1的素因数 q 必是$a+1$的因数，或是$q\equiv1\pmod{2p}$；

(iii) 形如$2kp+1$的素数有无穷多个。

19. 设$b>1$，$n\geqslant1$。证明：$n|\phi(b^n-1)$。

20. 设$(a,10)=1$。证明：一定存在其十进位表示每位数均为 1 的正整数 n，使得$a|n$。此外，这样的 n 有无穷多个。

21. 证明：任一整数$a\neq0$必是这样的正整数 n 的因数，它的十进位表示仅由 1 和 0 两个数字组成。把1,0换成 2,0，或 3,0，…，或9,0结论仍成立，但换成其它两个数字则不成立。

22. 设a,r是正整数，$(a,r)=1$。证明：在算术数列 $a+kr$ $(k=0,1,2,\cdots)$中一定可以选出一个几何数列来。

23. 设$m=2^l(l\geqslant3)$，$a=3$。求使 § 3式(17)成立的最小正整数$d=d_0$。进而，利用-1和 3，类似于定理 5 给出模2^l的既约剩余系。

24. 设 p 是素数，$a^p \equiv b^p \pmod p$。证明：$a^p \equiv b^p \pmod{p^2}$。

25. 证明：(i) $2^{10} \not\equiv 1 \pmod{11^2}$，$3^{10} \equiv 1 \pmod{11^2}$；

(ii) $2^{1092} \equiv 1 \pmod{1093^2}$，$3^{1092} \not\equiv 1 \pmod{1093^2}$。

26. 证明

$$\phi(n) = \sum_{l=1}^{n} \prod_{p \mid n} \left(1 - \frac{1}{p} \sum_{a=1}^{p} e^{2\pi i l a / p}\right).$$

§ 4 Wilson定理

定理1 (Wilson) 设 p 是素数，$r_1, \cdots, r_{p-1}$ 是模 p 的既约剩余系，我们有

$$\prod_{r \bmod p}{}' r \equiv r_1 \cdots r_{p-1} \equiv -1 \pmod p. \tag{1}$$

特别地有

$$(p-1)! \equiv -1 \pmod p) \text{①}. \tag{2}$$

证 当 $p=2$ 时结论显然成立。所以可设 $p \geqslant 3$。由 § 1 性质 VII 及其后的说明知，对取定的这一组既约剩余系中的每个 r_i 必有唯一的一个 r_j 使得

$$r_i r_j \equiv 1 \pmod p. \tag{3}$$

使 $r_i = r_j$ 的充要条件是

$$r_i^2 \equiv 1 \pmod p.$$

即

$$(r_i - 1)(r_i + 1) \equiv 0 \pmod p.$$

由于 p 是素数且 $p \geqslant 3$，所以上式成立当且仅当

$$r_i - 1 \equiv 0 \pmod p \quad \text{或} \quad r_i + 1 \equiv 0 \pmod p.$$

由于素数 $p \geqslant 3$，所以，这两式不能同时成立。因此，在这组模 p 的既约剩余系中，除了

---

① 习题一第25题提出了另一证明。

$$r_i \equiv 1,\ -1 \pmod p \tag{4}$$

这两个数外，对其它的r_i必有$r_j \neq r_i$使式(3)成立。不妨设$r_1 \equiv 1 \pmod p$，$r_{p-1} \equiv -1 \pmod p$。这样，在这组模$p$的既约剩余系中除去满足式(4)的两个数之外，其它的数恰好可按关系式(3)两两分完，即有

$$r_2 \cdots r_{p-2} \equiv 1 \pmod p.$$

由此就推出式(1)。$1,2,\cdots,p-1$是模p的既约剩余系，所以式(2)成立。证毕。

例如，对$p=13$。取$r_j=j(1\leqslant j\leqslant 12)$，我们有

$$2\cdot 7 \equiv 3\cdot 9 \equiv 4\cdot 10 \equiv 5\cdot 8 \equiv 6\cdot 11 \equiv 1 \pmod{13}.$$

所以式(2)（$p=13$）成立。仔细分析定理1的证明，可以看出，当p为奇素数时，以模$p^l(l\geqslant 2)$代替模p，所有的论证全部成立。由此可得以下定理(具体推导留给读者)。

定理 2 设素数$p\geqslant 3$，$l\geqslant 1$。$c=\phi(p^l)$，以及$r_1,r_2,\cdots,r_c$是模p^l的一组既约剩余系。我们有

$$r_1\cdot r_2\cdots r_c \equiv -1 \pmod{p^l}. \tag{5}$$

特别的有

$$\prod_{r=1}^{p-1}\prod_{s=0}^{p^{l-1}-1}(r+ps) \equiv -1 \pmod{p^l}. \tag{6}$$

例如，对$m=3^3$。$1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26$是一组模$3^3$的既约剩余系。我们有

$$2\cdot 14 \equiv 4\cdot 7 \equiv 5\cdot 11 \equiv 8\cdot 17 \equiv 10\cdot 19$$
$$\equiv 13\cdot 25 \equiv 16\cdot 22 \equiv 20\cdot 23 \equiv 1 \pmod{3^3}.$$

所以式(5)和(6)($p=3,l=3$)成立。

在定理2的符号和条件下，我们有(为什么)

$$c=\phi(p^l)=\phi(2p^l).$$

现取

$$r'_j=\begin{cases} r_j, & \text{当}2\nmid r_j, \\ r_j+p^l, & \text{当}2\mid r_j. \end{cases}$$

显见，$r'_j(1\leqslant j\leqslant c)$仍是模$p^l$的一组既约剩余系，且都是奇数。因此它也是模$2p^l$的一组既约剩余系，且有（为什么）

$$r'_1\cdots r'_c\equiv -1(\mathrm{mod}\,2p^l).$$

这样我们就证明了

定理3 设素数$p\geqslant 3$，$l\geqslant 1$，$c=\phi(2p^l)$，以及$r_1,\cdots,r_c$是模$2p^l$的一组既约剩余系。我们有

$$r_1\cdot r_2\cdots r_c\equiv -1(\mathrm{mod}\ 2p^l). \tag{7}$$

最后来证明：

定理4 设$c=\phi(2^l)=2^{l-1}$，$l\geqslant 1$，$r_1,\cdots,r_c$是模2^l的既约剩余系。我们有

$$r_1\cdots r_c\equiv\begin{cases}-1\ (\mathrm{mod}\ 2^l), & l=1,2,\\ 1\ (\mathrm{mod}\ 2^l), & l\geqslant 3.\end{cases} \tag{8}$$

证 $l=1,2$时结论可直接验证。现设$l\geqslant 3$。同样由§1性质Ⅷ及其后的说明知，对每个r_i必有唯一的r_j使

$$r_ir_j\equiv 1(\mathrm{mod}\ 2^l). \tag{9}$$

$r_i=r_j$的充要条件是

$$r_i^2\equiv 1(\mathrm{mod}\ 2^l),$$

即

$$(r_i-1)(r_i+1)\equiv 0(\mathrm{mod}\ 2^l).$$

注意到$(r_i,2)=1$，上式即

$$\frac{r_i-1}{2}\cdot\frac{r_i+1}{2}\equiv 0(\mathrm{mod}\ 2^{l-2}).$$

注意到：

$$\left(\frac{r_i-1}{2},\ \frac{r_i+1}{2}\right)=1,$$

就推出$r_i=r_j$的充要条件是

$$\frac{r_i-1}{2}\equiv 0(\mathrm{mod}\ 2^{l-2})\ \text{或}\ \frac{r_i+1}{2}\equiv 0(\mathrm{mod}\ 2^{l-2}),$$

即

$$r_i\equiv 1(\mathrm{mod}\ 2^{l-1})\ \text{或}\ r_i\equiv -1(\mathrm{mod}\ 2^{l-1}).$$

因此，在这个模2^l的既约剩余系中仅当

$$r_i \equiv 1, \quad 2^{l-1}-1, \quad 2^{l-1}-1 \text{ 或 } 2^l-1 \pmod{2^l} \qquad (10)$$

时，才可能有$r_i=r_j$。这样，对模2^l的既约剩余系中的每个r_i除去这四个数(这四个数两两对模2^l不同余)外，必有$r_j \neq r_i$。所以除了这四个数外，既约剩余系中的$c-4$个数可按关系式(9)两两分对分完，即这$c-4$个数的乘积对模2^l同余于1．由此及式(10)就证明了式(8)对$l \geqslant 3$成立。

总结以上讨论，我们证明了当$m=1,2,4,p^l,2p^l$(p为奇素数)时，模m的一组既约剩余系的乘积同余-1模m。可以证明在其它情形必同余于1模m。这将安排在习题中。

Wilson定理是很有用的．下面来举两个例子．

例1 设$r_0,r_1,\cdots,r_{p-1}$及$r'_0,r'_1,\cdots,r'_{p-1}$是模$p$的两组完全剩余系，$p$是奇素数。证明：$r_0r'_0,r_1r'_1,\cdots,r_{p-1}r'_{p-1}$一定不是模$p$的完全剩余系。

证 用反证法．假设$r_0r'_0,r_1r'_1,\cdots,r_{p-1}r'_{p-1}$是模$p$的完全剩余系，那么，其中有且仅有一个被$p$整除，不妨设

$$p|r_0r'_0, \quad p \nmid r_jr'_j, \quad 1 \leqslant j \leqslant p-1.$$

因此，必有(为什么)

$$p|r_0, p|r'_0, \quad p \nmid r_j, \quad p \nmid r'_j, \quad 1 \leqslant j \leqslant p-1.$$

所以，$r_1,\cdots,r_{p-1}$及$r'_1,\cdots,r'_{p-1}$都是模p的既约剩余系，且$r_1r'_1,\cdots,r_{p-1}r'_{p-1}$也是模$p$的既约剩余系，我们来证明这是不可能的．因为，由定理1知

$$r_1\cdots r_{p-1} \equiv -1 \pmod p,$$
$$r'_1\cdots r'_{p-1} \equiv -1 \pmod p$$

以及

$$(r_1r'_1)\cdots(r_{p-1}r'_{p-1}) \equiv -1 \pmod p.$$

但前两式相乘得

$$(r_1r'_1)\cdots(r_{p-1}r'_{p-1}) \equiv 1 \pmod p.$$

因而有

$$1\equiv -1 \pmod p.$$

但 $p\geqslant 3$ 这是不可能．这就证明了所要的结论．

例 2　设 p 是奇素数，证明

$$1^2\cdot 3^2\cdots(p-2)^2\equiv(-1)^{(p+1)/2} \pmod p.$$

证　注意到当 p 为奇素数时

$$\begin{aligned}(p-1)!&=(1\cdot(p-1))(3\cdot(p-3))\cdots((p-4)(p-(p-4)))\\&\quad\cdot((p-2)(p-(p-2)))\\&\equiv(-1)^{(p-1)/2}\cdot 1^2\cdot 3^2\cdots(p-2)^2 \pmod p,\end{aligned}$$

由此及定理 1 即得所要结论．

习　题　四

1．证明：n 是素数的充要条件是：

(i) $n\mid(n-1)!+1$；(ii) $n\mid(n-2)!-1$；

(iii) 存在正整数 $k\leqslant n$，使得 $n\mid(k-1)!(n-k)!+(-1)^{k-1}$．

2．设素数 $p>5$．证明：(i) $(p-1)!+1$ 不可能是素数的方幂；(ii) $(p-2)!-1$ 不可能是素数的方幂．

3．证明 $n, n+2$ 同时是素数的充要条件是：

$$4((n-1)!+1)\equiv -n(\bmod\ n(n+2)).$$

4．设 p 是奇素数．证明：

(i) $2^2\cdot 4^2\cdots(p-1)^2\equiv(-1)^{(p+1)/2} \pmod p$；

(ii) $(((p-1)/2)!)^2\equiv(-1)^{(p+1)/2} \pmod p$；

(iii) $(p-1)!!\equiv(-1)^{(p-1)/2}(p-2)!! \pmod p$

5．设 p 为素数，a 为任意整数．证明：

(i) $p\mid a^p+(p-1)!a$；(ii) $p\mid(p-1)!a^p+a$．

6．设素数 p 为奇数．证明：

(i) 当 $p=4m+3$ 时，对任意整数 a 均有 $a^2\not\equiv -1 \pmod p$；

(ii) 当 $p=4m+1$ 时，必有 a 满足 $a^2\equiv -1 \pmod p$．进而推出：

(iii) 形如 $4m+1$ 的素数有无穷多个。

7. 设 $m=4, p^\alpha, 2p^\alpha$，p 为奇素数，$\alpha\geqslant1$。再设 $r_1,\cdots,r_c$，及 $r'_1,\cdots,r'_c$ 是模 m 的两组既约剩余系。证明：$r_ir'_i(1\leqslant i\leqslant c)$一定不是模 m 的既约剩余系。

8. 设$m=4, p^\alpha, 2p^\alpha$，p 为奇素数，$\alpha\geqslant1$。再设 $r_1,\cdots,r_m$ 及$r'_1,\cdots,r'_m$ 是模 m 的两组完全剩余系。证明：$r_ir'_i(1\leqslant i\leqslant m)$一定不是模 m 的完全剩余系。

9. 设 $r_1,\cdots,r_4$ 及 $r'_1,\cdots,r'_4$ 是模 8 的两组既约剩余系。$r_1r'_1,\cdots,r_4r'_4$ 是否一定不是模 8 的既约剩余系？举例说明。对模 15 的两组既约剩余系作同样的讨论。

10. 设 $m\geqslant3, r_1,\cdots,r_m$ 及 $r'_1,\cdots,r'_m$ 是模 m 的两组完全剩余系。证明：$r_1r'_1,\cdots,r_mr'_m$ 一定不是模 m 的完全剩余系（提示：利用§3定理 2 的证明二中的方法，及本节例 1）。

11. 设 $m\neq1,2,4,p^\alpha,2p^\alpha$，$p$ 为奇素数。证明：

$$\prod_{r \bmod m}{}' r\equiv1(\bmod m),$$

即任意一组模 m 的既约剩余系的元素的乘积同余 1 模 m（提示：利用§2定理15）。

第四章 同余方程

同余方程是同余理论的核心内容，本章仅介绍它的一些基本知识。§1中介绍有关同余方程的基本概念和术语；§2和§3讨论一次同余方程与一次同余方程组，证明了著名的孙子定理——实际上它也是刻画了剩余系的整体性质（见第三章§2）；高于一次的同余方程在理论上至今也没有得到多少结果，§4中介绍求解一般同余方程的具体算法；§5，§6与§7讨论模为素数的二次同余方程的性质，引进了二次剩余、二次非剩余的概念及Legendre符号。判断模为素数的二次同余方程是否有解就归结为计算Legendre符号，我们证明了关于Legendre符号的著名的Gauss二次互反律，利用这一定理就解决了Legendre符号的计算。利用Jacobi符号的性质就能更方便地计算Legendre符号；最后，在§8对模为素数的高次同余方程的解数得到了一些理论上的结果，证明了Lagrange定理。特别讨论了模为素数的二项同余方程，介绍了模为素数的n次剩余与n次非剩余的概念。

§1 同余方程的基本概念

设整系数多项式

$$f(x)=a_nx^n+\cdots+a_1x+a_0, \tag{1}$$

我们把含有变数x的同余式

$$f(x)\equiv 0 \pmod m \tag{2}$$

称为是模m的同余方程。若整数c满足

$$f(c)\equiv 0 \pmod m,$$

则称c是同余方程(2)的解，显见，这时同余类$c \bmod m$中的任一

整数也是同余方程(2)的解，我们把这些解都看作是相同的，也常说同余类 $c \bmod m$ 是同余方程(2)的一个解，我们写为

$$x\equiv c(\bmod m)$$

是同余方程(2)的解。当 c_1, c_2 均为同余方程(2)的解，且对模 m 不同余时才把它们看作是同余方程(2)的不同的解。我们把所有对模 m 两两不同余的(2)的解的个数称为是同余方程(2)的解数。因此，我们只要**在模 m 的一组完全剩余系中来解模 m 的同余方程**。显然，**模 m 的同余方程的解数至多为 m**。

例 1 求同余方程 $4x^2+27x-12\equiv 0(\bmod 15)$ 的解。

解 取模 15 的绝对最小完全剩余系：$-7, -6, \cdots, -1, 0, 1, 2, \cdots, 7$。直接计算知 $x=-6, 3$ 是解。所以，这个同余方程的解是

$$x\equiv -6, 3(\bmod 15),$$

解数为 2。

例 2 求同余方程 $4x^2+27x-7\equiv 0(\bmod 15)$ 的解。

同样直接计算知 $x=-7, -2, -1, 4$ 是解。所以它的解是

$$x\equiv -7, -2, -1, 4(\bmod 15),$$

解数为 4。

例 3 求解同余方程 $4x^2+27x-9\equiv 0(\bmod 15)$。

直接计算知，这方程无解。

当 $f(x)$ 的系数都是模 m 的倍数时，显见，任意的整数值 x 都是同余方程(2)的解，这样的同余方程(2)的解数为 m。但这并不是同余方程(2)的解数为 m 的必要条件，这可由下面的例子看出。

例 4 由第三章 §3 定理 3（Fermat-Euler 定理）知，同余方程

$$x^5-x\equiv 0(\bmod 5) \tag{3}$$

的解数为 5；同余方程

$$x^7-x\equiv 0(\bmod 7) \tag{4}$$

的解数为 7；以及同余方程

$$x(x^2-1)(x^2+1)(x^4+x^2+1)\equiv 0 \pmod{35},$$

即

$$x^9+x^7-x^3-x\equiv 0 \pmod{35} \tag{5}$$

的解数为 35（为什么），一般的，对素数 p，同余方程

$$x^p-x\equiv 0 \pmod{p} \tag{6}$$

的解数为 p。

如同为了解代数方程需要对代数方程进行恒等变形一样，为了解同余方程需要利用同余式的性质对同余方程进行恒等变形，使它变得尽可能的简单。最基本、最简单的有以下几种（证明留给读者）：

（Ⅰ）设 $s(x)$ 是整系数多项式。同余方程(2)和同余方程

$$f(x)+ms(x)\equiv 0 \pmod{m} \tag{7}$$

等价，即它们的解和解数相同。利用第三章 § 1式(5)的符号，这一恒等变形可表述为：若

$$f(x)\equiv g(x) \pmod{m},$$

则同余方程(2)和同余方程

$$g(x)\equiv 0 \pmod{m} \tag{8}$$

的解和解数相同。例如，例 1 中的同余方程和

$$4x^2-3x+3\equiv 0 \pmod{15}, \tag{9}$$

或

$$4x^2+12x-12\equiv 0 \pmod{15} \tag{10}$$

都是等价的。特别地，一个同余方程中系数为模的倍数的项去掉后，同余方程的解不变。例如，同余方程

$$15x^8+7x^6+45x^3-30x+6\equiv 0 \pmod{15} \tag{11}$$

可化简为

$$7x^6+6\equiv 0 \pmod{15}. \tag{12}$$

由此，可引进同余方程的次数的概念：若 $m\nmid a_n$，则称模 m 的同余方程(2)的次数为 n。一般的，若 $m|a_j, k+1\leqslant j\leqslant n, m\nmid a_k$，则称模 m 的同余方程(2)的次数为 k。当 $m|a_j (0\leqslant j\leqslant n)$ 时，我们就不

说同余方程(2)的次数。例 1—例 3 中的同余方程都是二次的；同余方程(3)，(4)，(5)及(6)的次数分别为五次，七次，九次及 p 次。同余方程(11)的次数为 6 。对同余方程

$$45x^7-30x^3+15x+105\equiv0\pmod{15}$$

就不说它的次数。要特别注意的是：同余方程 (2) 的次数和多项式 $f(x)$ 的次数不是一回事。

(Ⅱ) 设 $s(x)$是整系数多项式．同余方程(2)与同余方程

$$f(x)+s(x)\equiv s(x)\pmod{m} \tag{13}$$

的解和解数相同。例如，例 1 中的同余方程与

$$4x^2+27x\equiv12\pmod{15}$$

是一样的。同余方程

$$ax-b\equiv0\pmod{m}$$

和同余方程

$$ax\equiv b\pmod{m}$$

是一样的，经常利用的是后一形式。当 $m\nmid a$ 时，这是一次同余方程。

(Ⅲ) 设$(a,m)=1$，同余方程(2)与同余方程

$$af(x)\equiv0\pmod{m}$$

的解和解数相同。例如，同余方程(10)与同余方程

$$x^2+3x-3\equiv0\pmod{15}$$

一样。

利用恒等变形(Ⅰ)和(Ⅲ)可得到以下结论：

定理1 若$(a_n,m)=1$及

$$a_n^{-1}a_n\equiv1\pmod{m},$$

则同余方程(2)与同余方程

$$x^n+a_n^{-1}a_{n-1}x^{n-1}+\cdots+a_n^{-1}a_1x+a_n^{-1}a_0\equiv0\pmod{m} \tag{14}$$

的解和解数一样。

请读者自己写出详细证明。这性质是经常要用到的。

例如，同余方程(12)与同余方程

$$2\cdot(7x^6+6)\equiv 14x^6+12\equiv 0 \pmod{15}$$

一样；进而由恒等变形(Ⅰ)知，又与同余方程

$$-x^6-3\equiv 0 \pmod{15}$$

一样；再由恒等变形(Ⅲ)(取 $a=-1$)知，与同余方程

$$x^6+3\equiv 0 \pmod{15}$$

一样；利用恒等变形(Ⅱ)，可写为

$$x^6\equiv -3 \pmod{15}。$$

容易算出这同余方程无解（如何算）。

利用恒等同余式可化简同余方程。

(Ⅳ) 设同余方程

$$h(x)\equiv 0 \pmod{m} \tag{15}$$

的解数为 m，即上式是恒等同余式。如果整系数多项式 $q(x)$，$r(x)$ 满足

$$f(x)=q(x)h(x)+r(x), \tag{16}$$

或更一般地

$$f(x)\equiv q(x)h(x)+r(x) \pmod{m}, \tag{17}$$

那么，同余方程(2)与同余方程

$$r(x)\equiv 0 \pmod{m} \tag{18}$$

的解与解数相同。如果 $h(x)$ 的最高次项系数为1，那么，一定存在整系数多项式 $q(x)$ 与 $r(x)$，$r(x)$ 的次数小于 $h(x)$ 的次数，使得式(16)成立。

前一部分结论是显然的，后一部分只要利用多项式除法就可推出。显见，恒等变形(Ⅰ)是(Ⅳ)的特例。利用(Ⅳ)可降低同余方程的次数，关键是要找到模 m 的恒等同余式(15)，常用的是 m 为素数 p，及恒等同余式(6)。

例5 解同余方程

$$f(x)=2x^7-x^5-3x^3+6x+1\equiv 0 \pmod{5}。$$

解 利用恒等同余式(3)。由多项式除法得

$$f(x)=(2x^2-1)(x^5-x)-x^3+5x+1$$
$$\equiv(2x^2-1)(x^5-x)-x^3+1 \pmod 5.$$

所以原同余方程就化为

$$x^3\equiv 1 \pmod 5.$$

直接计算知，解为 $x\equiv 1 \pmod 5$。

最后，来给出一个显然而又十分有用的性质。

定理2 设正整数 $d\mid m$。那么同余方程(2)有解的必要条件是同余方程

$$f(x)\equiv 0 \pmod d \tag{19}$$

有解。

这是第三章 §1 性质V的直接推论。利用定理 2 可给出一个解一般同余方程的算法，这将在 §4讨论。定理 2 更常用来判定同余方程无解。例如，为判定例3 中的同余方程无解，只要讨论同余方程

$$4x^2+27x-9\equiv 0 \pmod 5.$$

利用恒等变形，它可化为

$$-x^2+2x+1\equiv 0 \pmod 5,$$

即

$$(x-1)^2\equiv 2 \pmod 5.$$

容易算出它无解，所以例3 中的方程无解。

习 题 一

1. 通过直接计算求下列同余方程的解和解数：

(i) $x^5-3x^2-2\equiv 0 \pmod 7$；

(ii) $3x^4-x^3+2x^2-26x+1\equiv 0 \pmod{11}$；

(iii) $3x^2-12x-19\equiv 0 \pmod{28}$；

(iv) $3x^2+18x-25\equiv 0 \pmod{28}$；

(v) $x^2+8x-13\equiv 0 \pmod{28}$；

(vi) $4x^2+21x-32\equiv 0 \pmod{141}$;

(vii) $x^{26}+7x^{21}-5x^{17}+2x^{11}+8x^5-3x^2-7\equiv 0 \pmod 5$;

(viii) $5x^{18}-13x^{12}+9x^7+18x^4-3x+8\equiv 0 \pmod 7$。

2. 设$(2a,m)=1$。证明：同余方程 $ax^2+bx+c\equiv 0 \pmod m$ 一定可化为$(dx+e)^2\equiv f \pmod m$。利用这一方法来解§1例1,2,3中的同余方程。

3. 设 p 是素数。证明：同余方程$f^2(x)\equiv 0 \pmod{p^{\alpha}}$与$f(x)\equiv 0 \pmod{p^{[(\alpha+1)/2]}}$的解相同。

4. 设 p 为素数。若 $g(x)\equiv 0 \pmod p$ 无解，则 $f(x)\equiv 0 \pmod p$ 与 $f(x)g(x)\equiv 0 \pmod p$的解与解数相同。

5. 以 $N(k)$ 记同余方程 $f(x)\equiv k \pmod m$ 的解数。证明：

$$\sum_{k=1}^{m} N(k)=m.$$

6. 对哪些值 a，同余方程 $x^3\equiv a \pmod 9$有解。

7. 求 $2^x\equiv x^2 \pmod 3$的解。

8. 求 $x^4+y^4\equiv 1 \pmod 5$的全部解$\{x,y\}$。

9. 证明：$x^3+y^3+z^3\equiv 0 \pmod 9$无 $3\nmid xyz$ 的解。

10. 证明：同余方程（2）一定可化为一个次数$<m$ 的多项式（包括系数均为m的倍数的情形）的同余方程。对合数模如何利用第三章§3习题三第15题来改进这一结果？

11. 证明：同余方程(2)的解数

$$T=\frac{1}{m}\sum_{l=0}^{m-1}\sum_{x=0}^{m-1} e^{2\pi i\, l f(x)/m}.$$

由此推出，当 $f(x)=ax-b$ 时，

$$T=\begin{cases}(a,m), & \text{当}(a,m)\mid b;\\ 0, & \text{当}(a,m)\nmid b.\end{cases}$$

12. 设 $f(x_1,\cdots,x_k)$是 $x_1,\cdots,x_k$ 的整系数多项式。证明：同余方程 $f(x_1,\cdots,x_k)\equiv 0 \pmod m$的解$\{x_1,\cdots,x_k\}$的个数

$$T=\frac{1}{m}\sum_{l=0}^{m-1}\sum_{x_1=0}^{m-1}\cdots\sum_{x_k=0}^{m-1}e^{2\pi i\, l f(x_1,\cdots,x_k)/m}$$

进而推出，当 $f(x_1,\cdots,x_k)=a_1x_1+\cdots+a_kx_k-b$ 时，

$$T=\begin{cases}m^{k-1}(a_1,\cdots,a_k,m), & 当(a_1,\cdots,a_k,m)\mid b;\\ 0, & 当(a_1,\cdots,a_k,m)\nmid b.\end{cases}$$

§2 一次同余方程

设 $m\nmid a$。这一节讨论最简单的模m的一次同余方程

$$ax\equiv b(\bmod m). \tag{1}$$

如果同余方程(1)有解 $x=x_1$，则有某个整数 y_1 使得

$$ax_1=b+my_1.$$

因此，(1)有解的必要条件是

$$(a,m)\mid b. \tag{2}$$

例如，同余方程

$$4x\equiv 2(\bmod 8)$$

一定无解，因为$(4,8)=4\nmid 2$。同余方程

$$3x\equiv 2(\bmod 8)$$

满足条件(2)，因为$(3,8)=1$。在模 8 的绝对最小完全剩余系 -3，-2，-1，0，1，2，3，4 中，x 逐一取值验算知，仅有解 $x=-2$，即其解为 $x\equiv-2(\bmod 8)$，解数为 1 。同余方程

$$6x\equiv 2(\bmod 8)$$

也满足条件(2)，因为 $(6,8)=2\mid 2$。同样，x 逐一取值验算知，$x=-1,3$ 是解，即这同余方程的解是

$$x\equiv-1,3(\bmod 8),$$

解数为 2 。

定理1 当$(a,m)=1$时，同余方程(1)必有解，且其解数为1。

证法一 由第三章§2定理 10 知，当$(a,m)=1$时，x 遍历模

m 的一组完全剩余系时，ax 也遍历模 m 的完全剩余系，即若 $r_1,\cdots,r_m$ 是模 m 的一组完全剩余系，则 $ar_1,\cdots,ar_m$ 也是模 m 的一组完全剩余系。因此，有且仅有一个 $r_i=x_0$ 使得

$$ax_0\equiv ar_i\equiv b(\bmod m),$$

即同余方程(1)有且仅有一个解 $x\equiv x_0(\bmod m)$。

证法二① 当 $(a,m)=1$ 时，由第三章§1性质Ⅷ知，a 对模 m 有逆 a^{-1}（任取一个）满足

$$aa^{-1}\equiv 1(\bmod m).$$

容易看出

$$x_1=a^{-1}b$$

就满足同余方程(1)。若还有解 x_2，则有

$$ax_2\equiv ax_1(\bmod m),$$

由此从第三章§1性质Ⅶ推出

$$x_2\equiv x_1(\bmod m).$$

这就证明了解数为1。特别的，由第三章§3式(16)知，这时同余方程(1)的解是

$$x\equiv a^{\phi(m)-1}b(\bmod m). \qquad (3)$$

定理2 同余方程(1)有解的充要条件是式(2)成立。在有解时，它的解数等于 (a,m)，以及若 x_0 是(1)的解，则它的 (a,m) 个解是

$$x\equiv x_0+\frac{m}{(a,m)}\cdot t(\bmod m),$$

$$t=0,\cdots,(a,m)-1. \qquad (4)$$

证法一 当 $g=(a,m)=1$ 时，这就是定理1。所以可假定 $g>1$。必要性前面已经证明，下证充分性。若式(2)成立，则由第三章§1性质Ⅵ知，满足同余方程(1)的 x 的值和满足同余方程

$$\frac{a}{g}x\equiv\frac{b}{g}\left(\bmod \frac{m}{g}\right) \qquad (5)$$

---

① 这一证法实质上就是利用§1的恒等变形(Ⅱ)。

的 x 的值是相同的。由于 $(a/g, m/g)=1$，故由定理 1 知同余方程(5)有解，所以同余方程(1)也有解。这就证明了充分性。若 x_0 是同余方程(1)的解，则它也是同余方程(5)的解，进而由定理1知，满足同余方程(5)的所有的 x 的值是

$$x \equiv x_0 \left(\bmod \frac{m}{g}\right). \tag{6}$$

由上面讨论知，式(6)也给出了满足同余方程(1)的所有的 x 的值(不是解数)。由第三章§2 定理 4 的式(7)(取 $m_1=m/g, r=x_0, l=g$)知，由式(6)给出的模 m/g 的同余类 $x_0 \bmod (m/g)$ 就是以下 g 个模 m 的同余类之和：

$$\left(x_0+\frac{m}{g}t\right) \bmod m, \quad t=0, \cdots, g-1.$$

这就证明了定理的后一半结论。

证法二 我们通过讨论一次同余方程和一次不定方程的关系来证明定理。显见，同余方程(1)与不定方程

$$ax=my+b \tag{7}$$

同时有解或无解，且有解时满足这两个方程的 x 的值完全相同。由第二章§1 定理 1 知，不定方程(7)有解的充要条件是 $(a, m)=(a, -m) \mid b$。这就证明了定理的前一半结论。当同余方程(1)有解 x_0 时，不定方程(7)有解 x_0, y_0，这里

$$y_0=(ax_0-b)/m. \tag{8}$$

进而，由第二章§1定理 2 知，不定方程(7)的全部解为(注意正负号)：

$$x=x_0+\frac{m}{(a, m)}t, \quad y=y_0+\frac{a}{(a, m)}t,$$

$$t=0, \pm 1, \pm 2, \cdots. \tag{9}$$

由前面讨论知，满足同余方程(1)的所有的 x 的值为

$$x=x_0+\frac{m}{(a, m)}t, \quad t=0, \pm 1, \pm 2, \cdots. \tag{10}$$

这就是模 $m/(a,m)$ 的一个同余类

$$x_0 \bmod \frac{m}{(a,m)}.$$

由第三章§2定理4的式(7)(取 $m_1=m/(a,m)$, $r=x_0$, $d=g$)知，这个模 $m/(a,m)$ 的同余类就是式(4)给出的 (a,m) 个模 m 的同余类之和。这就证明了定理的后一半结论。

定理1和定理2不仅从理论上完全解决了同余方程(1)的求解问题，而且给出的不同的证法实际上是指出了具体求解的各种方法。下面来介绍一种直接求解同余方程(1)的算法，它类似于第二章§1例3中解二元一次不定方程的算法。

(i) 取 $a_1\equiv a \pmod m$, $-m/2<a_1\leqslant m/2$; $b_1\equiv b \pmod m$, $-m/2<b_1\leqslant m/2$。由§1恒等变形(Ⅰ)知，同余方程(1)就是同余方程

$$a_1x\equiv b_1 \pmod m. \tag{11}$$

(ii) 同余方程(11)与同余方程

$$my\equiv -b_1 \pmod{|a_1|} \tag{12}$$

同时有解或无解。这是因为由定理2的证法二中知，同余方程(11)与不定方程

$$a_1x=my+b_1$$

同时有解或无解，而这不定方程可写为

$$my=-b_1+a_1x.$$

同样理由，上述不定方程与同余方程(12)同时有解或无解。

(iii) 若 $y_0 \bmod |a_1|$ 是(12)的解，则 $x_0 \bmod m$ 是(11)，即(1)的解，这里

$$x_0=(my_0+b_1)/a_1. \tag{13}$$

反过来，若 $x_0 \bmod m$ 是(1)即(11)的解，则 $y_0 \bmod |a_1|$ 是(12)的解，这里

$$y_0=(a_1x_0-b_1)/m. \tag{14}$$

此外，若 $y_0 \bmod |a_1|$, $y_0' \bmod |a_1|$ 是(12)的两个不同的解，则相

应地确定的$x_0 \bmod m$，$x_0' \bmod m$也是(11)即(1)的两个不同的解。所以(12)和(11)即(1)的解数相同(请读者自己验证这些结论)。

以上的步骤(i)，(ii)，(iii)表明：求解模m的同余方程(1)，通过同余方程(11)转化为求解较小的模$|a_1|$的同余方程(12)。如果(12)能立即解出，则由(13)就得到(1)的全部解；如果(12)还不容易解出，则继续对它用步骤(i)，(ii)，化为一模更小的同余方程。这样进行下去总能使问题归结为求解一模很小且能直接看出其是否有解的同余方程。再依次利用式(13)(即步骤(iii))反回上去即可求得(1)的全部解。下面来举个具体例子。

例 1　解同余方程$589x\equiv 1026 \pmod{817}$。

$$589x\equiv 1026 \pmod{817} \overset{(i)}{\Longleftrightarrow} -228x\equiv 209 \pmod{817}$$

$$\overset{(ii)}{\Longleftrightarrow} 817y\equiv -209 \pmod{228} \overset{(i)}{\Longleftrightarrow} -95y\equiv 19 \pmod{228}$$

$$\overset{(ii)}{\Longleftrightarrow} 228z\equiv -19 \pmod{95} \overset{(i)}{\Longleftrightarrow} 38z\equiv -19 \pmod{95}$$

$$\overset{(ii)}{\Longleftrightarrow} 95w\equiv 19 \pmod{38} \overset{(i)}{\Longleftrightarrow} 19w\equiv 19 \pmod{38}$$

$$\overset{(ii)}{\Longleftrightarrow} 38u\equiv -19 \pmod{19} \overset{(i)}{\Longleftrightarrow} 0\cdot u\equiv 0 \pmod{19}.$$

这表明最后一个关于u的同余方程对模19有19个解：

$$u\equiv 0,1,2,\cdots,18 \pmod{19}.$$

按(iii)，即式(13)逐次反回上去得：关于w对模38的同余方程有19个解

$$w\equiv (38u+19)/19\equiv 2u+1 \pmod{38},$$

$$u=0,1,\cdots,18;$$

关于z对模95的同余方程有19个解：

$$z\equiv (95w-19)/38\equiv 5u+2 \pmod{95},$$

$$u=0,1,\cdots,18;$$

关于y对模228的同余方程有19个解：

$$y\equiv (228z+19)/(-95)\equiv -12u-5 \pmod{228},$$

$$u=0,1,\cdots 18;$$

最后得到 x 对模817的同余方程有19个解：

$$x \equiv (817y+209)/(-228) \equiv 43u+17 \pmod{817},$$

$$u=0,1,\cdots,18.$$

在运用这一方法时，千万不要把m, a_1, b_1搞错（特别是a_1的正负号）。此外，如果在运用这方法的过程中，利用同余式的性质化简同余方程时，改变了同余方程的模，则要注意方程的解数。例如，在例 1 中，当得到了同余方程

$$38z \equiv -19 \pmod{95} \tag{15}$$

后，如果利用第三章 § 1性质Ⅵ，就得到

$$2z \equiv -1 \pmod{5}.$$

容易看出，满足这同余方程的所有的 z 的值是

$$z \equiv 2 \pmod{5}.$$

但原来对 z 的同余方程的模为95，为了得到原方程(15)的解数，就要利用第三章 § 2定理 4 ，得到(15)有19个解：

$$z \equiv 2+5u,\quad u=0,1,\cdots,18.$$

这就是在例 1 中得到的。下面的做法和例 1 一样。

例 2　$21x \equiv 38 \pmod{117}$.

$$21x \equiv 38 \pmod{117}$$

$$\overset{\text{(ii)}}{\Longleftrightarrow} 117y \equiv -38 \pmod{21} \overset{\text{(i)}}{\Longleftrightarrow} -9y \equiv 4 \pmod{21}$$

$$\overset{\text{(ii)}}{\Longleftrightarrow} 21z \equiv -4 \pmod{9} \overset{\text{(i)}}{\Longleftrightarrow} 3z \equiv -4 \pmod{9}$$

$$\overset{\text{(ii)}}{\Longleftrightarrow} 9w \equiv 4 \pmod{3} \overset{\text{(i)}}{\Longleftrightarrow} 0\cdot w \equiv 1 \pmod{3},$$

最后的同余方程无解，所以原方程无解。

习　题　二

1．求解下列一元一次同余方程。

(i)　$3x \equiv 2 \pmod{7}$；

(ii)　$9x \equiv 12 \pmod{15}$；

(iii) $7x\equiv 1 \pmod{21}$；

(iv) $20x\equiv 4 \pmod{30}$；

(v) $17x\equiv 14 \pmod{21}$；

(vi) $64x\equiv 83 \pmod{105}$；

(vii) $128x\equiv 833 \pmod{1001}$；

(viii) $987x\equiv 610 \pmod{1597}$；

(ix) $57x\equiv 87 \pmod{105}$；

(x) $49x\equiv 5000 \pmod{999}$。

2．利用同余式的以下两个性质

(1) $a\equiv b \pmod m \Longleftrightarrow a\equiv b+mt \pmod m$；

(2) 当 $(c,m)=1$ 时，$ca\equiv cb \pmod m \Longleftrightarrow a\equiv b \pmod m$；

提出解下列同余方程的简单方法：

(i) $2^k x\equiv b \pmod m$，$(2,m)=1$；

(ii) $3^k x\equiv b \pmod m$，$(3,m)=1$。

3．用你提出的第2题中的方法来解：

(i) 第1题的(vi)和(vii)；

(ii) $256x\equiv 179 \pmod{337}$；

(iii) $1215x\equiv 560 \pmod{2755}$；

(iv) $1296x\equiv 1105 \pmod{2413}$。

4．设 a 是正整数，$a\nmid m$，以及 a_1 是 m 对模 a 的最小正剩余。证明：同余方程 $ax\equiv b \pmod m$ 的解一定是同余方程 $a_1x\equiv -b[m/a] \pmod m$ 的解。反过来对吗？举例说明。

5．你能利用上题提出一个解一元一次同余方程的方法吗？用你提出的方法来解(i) $6x\equiv 7 \pmod{23}$；(ii) $5x\equiv 1 \pmod{12}$。并指出应用这一方法时要注意什么？

6．设 $(a,m)=1$，x_1 是 $ax\equiv 1 \pmod m$ 的解。再设 k 是正整数，$y_k=1-(1-ax_1)^k$。证明：$a|y_k$，以及 $x_k=y_k/a$ 是同余方程 $ax\equiv 1 \pmod{m^k}$ 的解。

7．利用上题来解：(i) $3x\equiv 1 \pmod{125}$；

(ii) $5x\equiv1 \pmod{243}$。

8．设$(a,m)=1$，b是整数．再设$f(x)$是整系数多项式，

$$g(y)=f(ay+b)。$$

证明：同余方程$f(x)\equiv0 \pmod m$与$g(y)\equiv0 \pmod m$的解数相同。并指出如何从解出$f(x)\equiv0 \pmod m$的解来求出$g(y)\equiv0 \pmod m$的解。

9．利用上题来解§1中的例1，例2及例3。

10．如果你已经求出了同余方程$ax\equiv b \pmod m$的解，那么，如何由此求出不定方程$ax+my=b$的解？以第1题的(i)，(iii)，(v)，(vii)题为例，来说明如何求相应的不定方程的解。

§3　一次同余方程组，孙子定理

在讨论一次同余方程组之前，先引进一般同余方程组的解与解数的概念。设$f_j(x)$是整系数多项式$(1\leqslant j\leqslant k)$。我们把含有变数$x$的一组同余式

$$f_j(x)\equiv0 \pmod{m_j},\quad 1\leqslant j\leqslant k, \tag{1}$$

称为是**同余方程组**．若整数c同时满足

$$f_j(c)\equiv 0 \pmod{m_j},\quad 1\leqslant j\leqslant k,$$

则称c是**同余方程组(1)的解**，显见，这时同余类

$$c \bmod m,\quad m=[m_1,\cdots,m_k] \tag{2}$$

中的任一整数也是同余方程组(1)的解，我们把这些解都看作是相同的，也常说同余类(2)是同余方程组的一个解，我们写为：

$$x\equiv c \pmod m$$

是同余方程组(1)的解。当c_1,c_2均为同余方程组(1)的解且对模m不同余时才把它们看作是同余方程组(1)的不同的解．我们把所有对模m两两不同余的同余方程组(1)的解的个数称为是**同余方程组(1)的解数**．因此，我们只要在模m的一组完全剩余系中

来求解同余方程组(1)，它的解数至多为m。此外，只要同余方程组(1)中的任意一个同余方程无解，则(1)一定无解。

定理1(孙子定理)　设$m_1,\cdots,m_k$是两两既约的正整数。那么，对任意整数$a_1,\cdots,a_k$，一次同余方程组

$$x\equiv a_j \pmod{m_j},\quad 1\leqslant j\leqslant k, \tag{3}$$

必有解，且解数为1。事实上，同余方程组(3)的解是

$$x\equiv M_1M_1^{-1}a_1+\cdots+M_kM_k^{-1}a_k \pmod{m}, \tag{4}$$

这里$m=m_1\cdots m_k$，$m=m_jM_j\ (1\leqslant j\leqslant k)$，以及$M_j^{-1}$是满足

$$M_jM_j^{-1}\equiv 1 \pmod{m_j},\quad 1\leqslant j\leqslant k \tag{5}$$

的一个整数(即是M_j对模m_j的逆)①。

证法一　由于$m_1,\cdots,m_k$两两既约，所以

$$m=[m_1,\cdots,m_k]=m_1\cdots m_k. \tag{6}$$

先来证若同余方程组(3)有解c_1,c_2，则必有

$$c_1\equiv c_2 \pmod{m}.$$

这因为当c_1,c_2均是同余方程组(3)的解时，必有

$$c_1\equiv c_2 \pmod{m_j},\quad 1\leqslant j\leqslant k.$$

由于$m_1,\cdots,m_r$两两既约，利用第三章§1性质Ⅸ，从上式及式(6)就推出所要的结论。这就证明了同余方程组(3)若有解则解数为1。下面来证由式(4)中给出的

$$c=M_1M_1^{-1}a_1+\cdots+M_kM_k^{-1}a_k \tag{7}$$

确是同余方程组(3)的解。显见，$(m_j,M_j)=1$，所以满足式(5)的M_j^{-1}必存在。由式(5)及$m_j\mid M_i,\ j\neq i$，就推出

$$c\equiv M_jM_j^{-1}a_j\equiv a_j \pmod{m_j},\quad 1\leqslant j\leqslant k,$$

即c是解。证毕。

证法一虽然简单，但为什么有形式(4)的解则看不清楚。下面来给出另一证法。

---

① 这里$M_1^{-1},\cdots,M_k^{-1}$只要取定一个整数，对不同的取值，式(4)表面上含有不同的值，但对模m是同余的。

证法二 为简单起见考虑 $k=2$ 的 情 形，现在，$m=m_1m_2$，$M_1=m_2$，$M_2=m_1$，及同余方程组(3)是

$$\begin{cases} x\equiv a_1(\bmod m_1), \\ x\equiv a_2(\bmod m_2). \end{cases} \tag{8}$$

由第一个方程知，可把 x 表为

$$x=a_1+m_1y. \tag{9}$$

这样，同余方程组(8)变为同余方程

$$m_1y\equiv a_2-a_1(\bmod m_2),$$

即

$$M_2y\equiv a_2-a_1(\bmod m_2).$$

由 §2定理 1 的证法二知

$$y\equiv M_2^{-1}(a_2-a_1)(\bmod m_2).$$

进而有

$$m_1y\equiv M_2M_2^{-1}(a_2-a_1)(\bmod m).$$

由此及式(9)得

$$\begin{aligned} x&\equiv a_1+M_2M_2^{-1}(a_2-a_1)(\bmod m) \\ &\equiv(1-M_2M_2^{-1})a_1+M_2M_2^{-1}a_2(\bmod m). \end{aligned} \tag{10}$$

由 m_1,m_2 的对称性，同样可得

$$x\equiv M_1M_1^{-1}a_1+(1-M_1M_1^{-1})a_2(\bmod m). \tag{11}$$

但式(10),(11)还都不是我们需要的式(4)($k=2$)的形式．但利用式(5)($k=2$)，容易看出

$$M_1M_1^{-1}\equiv 1-M_2M_2^{-1}(\bmod m_1),$$

$$M_1M_1^{-1}\equiv 1-M_2M_2^{-1}(\bmod m_2).$$

所以

$$M_1M_1^{-1}\equiv 1-M_2M_2^{-1}(\bmod m).$$

由此及式(10)(或(11))立即推出：若 x 是解则必有

$$x\equiv M_1M_1^{-1}a_1+M_2M_2^{-1}a_2(\bmod m).$$

容易验证 $M_1M_1^{-1}a_1+M_2M_2^{-1}a_2$ 的确是同余方程组(8)的解．证毕．

用证法二来证 $k>2$ 的情形并不方便．下面再介绍一种证法．

证法三　首先，我们来指出这样一个事实：若x_0满足同余方程组(3)，x'_0 满足下面的同余方程组

$$x\equiv a'_j \pmod{m_j},\quad 1\leqslant j\leqslant k,$$

那么，$x_0+x'_0$一定是同余方程组

$$x\equiv a_j+a'_j \pmod{m_j},\quad 1\leqslant j\leqslant k$$

的解。因此，我们可以用下面的叠加方法来求同余方程组(3)的解。设

$$a_j^{(i)}=\begin{cases}a_j, & i=j,\\ 0, & i\neq j.\end{cases} \tag{12}$$

对每个固定的$i(1\leqslant i\leqslant k)$考虑同余方程组

$$x\equiv a_j^{(i)} \pmod{m_j},\quad 1\leqslant j\leqslant k. \tag{13}$$

注意到$j\neq i$时 $a_j^{(i)}=0$，所以由这方程组的第$1,\cdots,i-1,i+1,\cdots,k$个方程知(注意 m_j 两两既约)

$$x\equiv 0 \pmod{M_i},$$

即

$$x=M_i y. \tag{14}$$

代入第 i 个方程得

$$M_i y\equiv a_i \pmod{m_i}.$$

由§2定理 1 的证法二知

$$y\equiv M_i^{-1}a_i \pmod{m_i},$$

即

$$M_i y\equiv M_i M_i^{-1}a_i \pmod{m}.$$

由此及式(14)得

$$x\equiv M_i M_i^{-1}a_i \pmod{m}.$$

容易验证，$M_iM_i^{-1}a_i$ 确是同余方程组(13)的解(这就是证明了同余方程组(13)有解且解数为1)。注意到由式(12)可得

$$a_j^{(1)}+a_j^{(2)}+\cdots+a_j^{(r)}=a_j,$$

所以，$M_1M_1^{-1}a_1+\cdots+M_kM_k^{-1}a_k$一定是同余方程组(3)的解。在

证法一中已证明了若有解，则解数必为1。定理证毕。

第一章§3的例2实际就是解同余方程组的例子，比如其中的(iii)就是说同余方程组

$$\begin{cases} x\equiv 0 \pmod 2, \\ x\equiv 1 \pmod 3) \end{cases}$$

的解是

$$x\equiv 4 \pmod 6.$$

大约在公元5～6世纪，我国南北朝时期有一部著名的算术著作《孙子算经》，其中有这样一个“物不知数”问题：“今有物，不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”这就是要求同余方程组

$$\begin{cases} x\equiv 2 \pmod 3, \\ x\equiv 3 \pmod 5, \\ x\equiv 2 \pmod 7) \end{cases} \tag{15}$$

的正整数解。书中求出了满足这一问题的最小正整数解$x=23$，所用的具体解法实质上就是求这同余方程组的形如式(4)的解。因此，把定理1称为**孙子剩余定理**。国际上称为**中国剩余定理**。我们来解同余方程组(15)，这里

$$m_1=3,\ \ m_2=5,\ \ m_3=7,$$

$$M_1=35,\ \ M_2=21,\ \ M_3=15.$$

容易算出可取$M_1^{-1}=2$，$M_2^{-1}=1$，$M_3^{-1}=1$。因此(15)的解为

$$\begin{aligned} x&\equiv 35\cdot 2\cdot 2+21\cdot 1\cdot 3+15\cdot 1\cdot 2 \\ &\equiv 233\equiv 23 \pmod{105}. \end{aligned}$$

因此，满足“物不知数”问题的正整数解是

$$x=23+105t,\ \ t=0,1,2,\cdots,$$

最小的为23。

孙子定理是数论中最重要的基本定理之一。它实质上刻画了剩余系的结构(我们已在第三章§2中讨论过)。设c由式(7)给出，

$$c' = M_1M_1^{-1}a'_1 + \cdots + M_kM_k^{-1}a'_k. \qquad (16)$$

容易证明：

$$c \equiv c' \pmod m$$

的充要条件是

$$a_j \equiv a'_j \pmod{m_j}, \quad 1 \leqslant j \leqslant k,$$

c 和 m 既约的充要条件是 a_j 和 m_j 都既约。因此，由孙子定理立即推出：

定理2 设 $m_1, \cdots, m_k, m, M_1, \cdots, M_k, M_1^{-1}, \cdots, M_k^{-1}$ 同定理1。再设

$$x = M_1M_1^{-1}x^{(1)} + \cdots + M_kM_k^{-1}x^{(k)}. \qquad (17)$$

那么，x 遍历模 m 的完全(既约)剩余系的充要条件是 $x^{(j)}$ 分别遍历模 m_j 的完全(既约)剩余系，这里"遍历"的意义同第三章§2定理12(或定理14)。此外，还有

$$x \equiv x^{(j)} \pmod{m_j}, \quad 1 \leqslant j \leqslant k. \qquad (18)$$

具体论证留给读者。应该指出，定理2是第三章§2定理16的特殊形式(取 $a_j = M_j^{-1}$)。事实上，我们可以利用第三章§2定理15来证明孙子定理。因为同余方程组(3)的解只要在模 m 的一个完全剩余系中去找，所以可以假定同余方程组(3)有第三章§2式(20)形式的解，然后具体定出其中的每个 $x^{(j)}$ $(1 \leqslant j \leqslant k)$，就得到同余方程组(3)的解由式(4)给出。详细推导留给读者。

下面来举几个例。

例1 解同余方程组

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv -1 \pmod 5, \\ x \equiv 2 \pmod 7, \\ x \equiv -2 \pmod{11}. \end{cases}$$

解 取 $m_1 = 3$，$m_2 = 5$，$m_3 = 7$，$m_4 = 11$，满足定理1的条件。这时，$M_1 = 5 \cdot 7 \cdot 11, M_2 = 3 \cdot 7 \cdot 11, M_3 = 3 \cdot 5 \cdot 11$，$M_4 = 3 \cdot 5 \cdot 7$，

我们来求M_j^{-1}。由于$M_1\equiv(-1)\cdot(1)\cdot(-1)\equiv 1 \pmod 3$，所以

$$1\equiv M_1M_1^{-1}\equiv M_1^{-1} \pmod 3,$$

因此可取$M_1^{-1}=1$。由$M_2\equiv(-2)\cdot(2)\cdot 1\equiv 1 \pmod 5$知，

$$1\equiv M_2M_2^{-1}\equiv M_2^{-1} \pmod 5,$$

因此可取$M_2^{-1}=1$。由$M_3\equiv 3\cdot 5\cdot 4\equiv 4 \pmod 7$知，

$$1\equiv M_3M_3^{-1}\equiv 4M_3^{-1} \pmod 7,$$

因此可取$M_3^{-1}=2$。由$M_4\equiv 3\cdot 5\cdot 7\equiv 4\cdot 7\equiv 6 \pmod{11}$知，

$$1\equiv M_4M_4^{-1}\equiv 6M_4^{-1} \pmod{11},$$

因此可取$M_4^{-1}=2$，进而由定理1知同余方程组解为

$$x\equiv(5\cdot 7\cdot 11)\cdot 1\cdot 1+(3\cdot 7\cdot 11)\cdot 1\cdot(-1)+(3\cdot 5\cdot 11)\cdot 2\cdot 2 \\ +(3\cdot 5\cdot 7)\cdot 2\cdot(-2) \pmod{3\cdot 5\cdot 7\cdot 11},$$

即

$$x\equiv 385-231+660-420\equiv 394 \pmod{1155}.$$

例 2 求相邻的四个整数，它们依次可被$2^2,3^2,5^2$及7^2整除。

解 设这四个相邻整数是$x-1,x,x+1,x+2$。按要求应满足

$$x-1\equiv 0 \pmod{2^2},\quad x\equiv 0 \pmod{3^2},$$
$$x+1\equiv 0 \pmod{5^2},\quad x+2\equiv 0 \pmod{7^2}.$$

所以，这是一个解同余方程组问题，这里

$$m_1=2^2,\quad m_2=3^2,\quad m_3=5^2,\quad m_4=7^2$$

两两既约，满足定理1的条件，$M_1=3^25^27^2$，$M_2=2^25^27^2$，$M_3=2^23^27^2$，$M_4=2^23^25^2$。由$M_1\equiv 1\cdot 1\cdot 1\equiv 1 \pmod{2^2}$知，

$$1\equiv M_1M_1^{-1}\equiv M_1^{-1} \pmod{2^2},$$

因此可取$M_1^{-1}=1$。由$M_2\equiv 10^2\cdot 7^2\equiv 1\cdot 4\equiv 4 \pmod{3^2}$知

$$1\equiv M_2M_2^{-1}\equiv 4M_2^{-1} \pmod{3^2},$$

因此可取$M_2^{-1}=-2$。由$M_3\equiv 2^2\cdot 21^2\equiv 2^2\cdot 4^2\equiv -11 \pmod{5^2}$知，

$$1\equiv M_3M_3^{-1}\equiv -11M_3^{-1} \pmod{5^2},$$
$$2\equiv -22M_3^{-1}\equiv 3M_3^{-1} \pmod{5^2},$$

$$16\equiv 24M_5^{-1}\equiv -M_5^{-1}\pmod{5^2},$$

因此可取 $M_5^{-1}=9$。由 $M_4=(-13)(-24)\equiv 3\cdot 6\equiv 18\pmod{7^2}$ 知

$$1\equiv M_4M_4^{-1}\equiv 18M_4^{-1}\pmod{7^2},$$

$$3\equiv 54M_4^{-1}\equiv 5M_4^{-1}\pmod{7^2},$$

$$30\equiv 50M_4^{-1}\equiv M_4^{-1}\pmod{7^2},$$

因此可取 $M_4^{-1}=-19$。因而由定理 1 知

$$x\equiv 3^2\cdot 5^2\cdot 7^2\cdot 1\cdot 1+2^2\cdot 5^2\cdot 7^2\cdot(-2)\cdot 0+2^2\cdot 3^2\cdot 7^2\cdot 9\cdot(-1)$$
$$+2^2\cdot 3^2\cdot 5^2\cdot(-19)\cdot(-2)\pmod{2^2\cdot 3^2\cdot 5^2\cdot 7^2}.$$

$$x\equiv 11025-15876+34200\equiv 29349\pmod{44100}.$$

所以满足要求的四个相邻整数有无穷多组，它们是

$$29348+44100t,\ 29349+44100t,$$
$$29350+44100t,\ 29351+44100t,$$
$$t=0,\pm 1,\pm 2,\cdots.$$

最小的这样的四个相邻正整数是：

$$29348, 29349, 29350, 29351.$$

例 3　求模11的一组完全剩余系，使其中每个数被2,3,5,7除后的余数分别为1, −1, 1, −1.

解　在定理 2 中取 $m_1=2$，$m_2=3$，$m_3=5$，$m_4=7$，$m_5=11$，以及 $x^{(1)}=1$，$x^{(2)}=-1$，$x^{(3)}=1$，$x^{(4)}=-1$。这样，由定理 2 知，当 $x^{(5)}$ 遍历模11的完全剩余系时，

$$x=M_1M_1^{-1}-M_2M_2^{-1}+M_3M_3^{-1}-M_4M_4^{-1}+M_5M_5^{-1}x^{(5)}\tag{19}$$

就给出了所要求的完全剩余系。下面来求 M_j^{-1} $(1\leqslant j\leqslant 5)$。由 $M_1\equiv 1\pmod 2$ 知，

$$1\equiv M_1M_1^{-1}\equiv M_1^{-1}\pmod 2,$$

所以可取 $M_1^{-1}=1$。由 $M_2\equiv -1\pmod 3$ 知，

$$1\equiv M_2M_2^{-1}\equiv(-1)\cdot M_2^{-1}\pmod 3,$$

所以可取 $M_2^{-1}=-1$。由 $M_3\equiv 2\pmod 5$ 知，

$$1\equiv M_3M_3^{-1}\equiv 2M_3^{-1}\pmod 5,$$

所以可取 $M_3^{-1}=-2$。由 $M_4\equiv 1 \pmod 7$ 知，

$$1\equiv M_4M_4^{-1}\equiv M_4^{-1}\pmod 7,$$

所以可取 $M_4^{-1}=1$。由 $M_5\equiv 1\pmod{11}$ 知，

$$1\equiv M_5M_5^{-1}\equiv M_5^{-1}\pmod{11},$$

所以可取$M_5^{-1}=1$①。这样就得到

$$\begin{aligned} x &= 3\cdot5\cdot7\cdot11+2\cdot5\cdot7\cdot11+2\cdot3\cdot7\cdot11\cdot(-2)\\ &\quad -2\cdot3\cdot5\cdot11+2\cdot3\cdot5\cdot7x^{(5)}\\ &= 1155+770-924-330+210x^{(5)}\\ &= 671+210x^{(5)}=210(x^{(5)}+3)+41. \end{aligned}$$

具有这样性质的最小的正的模11的完全剩余系是：

$$41,\ 210+41,\ 210\cdot2+41,$$
$$210\cdot3+41,\ 210\cdot4+41,\ 210\cdot5+41,$$
$$210\cdot6+41,\ 210\cdot7+41,\ 210\cdot8+41,$$
$$210\cdot9+41,\ 210\cdot10+41.$$

例 4 解同余方程组

$$x\equiv3\pmod 8,\quad x\equiv11\pmod{20},\quad x\equiv1\pmod{15}.$$

解 这里 $m_1=8$，$m_2=20$，$m_3=15$不两两既约，所以不能直接用定理 1．容易看出，这同余方程组的解和同余方程组

$$\begin{cases} x\equiv3\pmod 8,\\ x\equiv11\pmod 4,\\ x\equiv11\pmod 5,\\ x\equiv1\pmod 5,\\ x\equiv1\pmod 3\end{cases}$$

的解相同．显见，满足第一个方程的 x 必满足第二个方程，而第三，四个方程是一样的．因此，原同余方程组和同余方程组

$$\begin{cases} x\equiv3\pmod 8,\\ x\equiv1\pmod 5,\\ x\equiv1\pmod 3\end{cases}\qquad(20)$$

① 事实上可以不求M_5^{-1}，在式(19)中$M_5M_5^{-1}x^{(5)}$这项可用$M_5x^{(5)}$代替(为什么)。

的解相同。同余方程组(20)满足定理1的条件。容易解出(留给读者)同余方程组(20)的解为

$$x\equiv -29 \pmod{120}.$$

注意到$[8,20,15]=120$，所以这也就是原同余方程组的解，且解数为1。

例4给出了模$m_1,\cdots,m_k$不是两两既约时，同余方程组(3)如何求解的具体例子。对于一般情形的解法原则上也是这样。这些讨论将放在习题中。

例5 解同余方程$19x\equiv 556 \pmod{1155}$。

解 这是一个一次同余方程，当然可以用§2的方法来解，这里我们把它化为模较小的一次同余方程组来解，这种办法有时是方便的。由于$1155=3\cdot5\cdot7\cdot11$，所以由第三章§1性质Ⅸ知，这个同余方程和同余方程组

$$19x\equiv 556 \pmod 3),\quad 19x\equiv 556 \pmod 5,$$

$$19x\equiv 556 \pmod 7,\quad 19x\equiv 556 \pmod{11}$$

的解相同。利用§1的恒等变形(Ⅰ)，这同余方程组就是

$$x\equiv 1 \pmod 3,\quad -x\equiv 1 \pmod 5,$$

$$-2x\equiv 3 \pmod 7,\ -3x\equiv 6 \pmod{11}.$$

进而，再利用§1的恒等变形(Ⅲ)和(Ⅰ)(即解出上述同余方程组中的第二,三,四个方程)，上述同余方程组就变为

$$x\equiv 1 \pmod 3,\quad x\equiv -1 \pmod 5,$$

$$x\equiv 2 \pmod 7,\quad x\equiv -2 \pmod{11}.$$

这同余方程组就可用定理1的方法来解。实际上，这就是我们的例1中的同余方程组，它的解是

$$x\equiv 394 \pmod{1155}.$$

这就是原同余方程的解。

例6 解同余方程组

$$x\equiv 3 \pmod 7,\quad 6x\equiv 10 \pmod 8.$$

解 这不是定理1中的同余方程组的形式。容易看出，第二

个同余方程有解且解数为 2（具体求解留给读者）：

$$x \equiv -1, 3 \pmod 8.$$

因此，原同余方程组的解就是以下两个同余方程组的解：

$$x \equiv 3 \pmod 7, \quad x \equiv -1 \pmod 8; \tag{21}$$

及

$$x \equiv 3 \pmod 7, \quad x \equiv 3 \pmod 8. \tag{22}$$

容易求出（留给读者），同余方程组(21)的解是 $x \equiv 31 \pmod{56}$；同余方程组(22)的解是$x \equiv 3 \pmod{56}$。所以，原同余方程组的解数为 2，其解为

$$x \equiv 3, 31 \pmod{56}.$$

例 7　解同余方程组

$$\begin{cases} 3x \equiv 1 \pmod{10}, \\ 4x \equiv 7 \pmod{15}. \end{cases}$$

解　利用解例 4 的方法。这同余方程组的解与同余方程组

$$\begin{cases} 3x \equiv 1 \pmod 2, \\ 3x \equiv 1 \pmod 5, \\ 4x \equiv 7 \pmod 3, \\ 4x \equiv 7 \pmod 5) \end{cases}$$

的解相同。但第二个同余方程$3x \equiv 1 \pmod 5$可化为$x \equiv 2 \pmod 5$，第四个同余方程 $4x \equiv 7 \pmod 5$ 可化为 $x \equiv -2 \pmod 5$，与 $x = 2 \pmod 5$矛盾，所以原同余方程组无解。

习　题　三

1．求解下列一元一次同余方程组。

(i) $x \equiv 1 \pmod 4$，$x \equiv 2 \pmod 3$，$x \equiv 3 \pmod 5$；

(ii) $x \equiv 4 \pmod{11}$，$x \equiv 3 \pmod{17}$；

(iii) $x \equiv 2 \pmod 5$，$x \equiv 1 \pmod 6$，$x \equiv 3 \pmod 7$，
　　$x \equiv 0 \pmod{11}$；

(iv) $3x\equiv 1 \pmod{11}$, $5x\equiv 7 \pmod{13}$;

(v) $3x\equiv 6 \pmod{10}$, $3x\equiv 10 \pmod{17}$;

(vi) $x\equiv 7 \pmod{10}$, $x\equiv 3 \pmod{12}$, $x\equiv 12 \pmod{15}$;

(vii) $x\equiv 6 \pmod{35}$, $x\equiv 11 \pmod{55}$, $x\equiv 2 \pmod{33}$.

(其中(i),(ii),(iv),(v) 用定理1的证法二中的方法来解)

2. 把同余方程化为同余方程组来解.

(i) $23x\equiv 1 \pmod{140}$;　　(ii) $17x\equiv 229 \pmod{1540}$.

3. 求所有被3,4,5除后余数分别为1,2,3的全体整数.

4. 有一个人每工作八天后休息两天. 有一次他在星期六、星期日休息, 问最少要几周后他可以在星期天休息.

5. 设 k 是任意给定的正整数. 证明: 一定存在 k 个相邻整数, 其中任何一个数都能被大于1的立方数整除.

6. 设 k 是给定的正整数, $a_1,\cdots,a_k$是两两既约的正整数. 证明:一定存在 k 个相邻整数,使得第 j 个数被a_j整除($1\leqslant j\leqslant k$).

7. 设 $(a,b)=1$, $c\neq 0$. 证明: 一定存在整数 n 使得

$$(a+bn,c)=1.$$

8. 设 $m_1,\cdots,m_k$两两既约. 那么, 同余方程组

$$a_jx\equiv b_j \pmod{m_j},\qquad 1\leqslant j\leqslant k$$

有解的充要条件是每一个同余方程 $a_jx\equiv b_j \pmod{m_j}$ 均可解, 即 $(a_j,m_j)\mid b_j$ ($1\leqslant j\leqslant k$). 当 $m_1,\cdots,m_k$不两两既约时这结论成立吗?

9. 证明: 同余方程组 $x\equiv a_j \pmod{m_j}$ ($j=1,2$) 有解的充要条件是 $(m_1,m_2)\mid(a_1-a_2)$, 若有解则对模$[m_1,m_2]$的解数为1.

10. 证明: 同余方程组 $x\equiv a_j \pmod{m_j}$ ($1\leqslant j\leqslant k$)有解的充要条件是 $(m_i,m_j)\mid(a_i-a_j)$ ($1\leqslant i\neq j\leqslant k$). 若有解则对模$[m_1,\cdots,m_k]$的解数为1.

11. 设 $m=[m_1,\cdots,m_k]$. 证明:

(i) 一定可找到一组正整数 $m_1',\cdots,m_k'$满足: $m_j'\mid m_j$($1\leqslant j\leqslant$

k)，$m'_1,\cdots,m'_k$两两既约，及 $m=m'_1\cdots m'_k$；

(ii) 若同余方程组 $x\equiv a_j \pmod{m_j}$ ($1\leqslant j\leqslant k$)有解，则它的解与同余方程组 $x\equiv a_j \pmod{m'_j}$ 的解相同。

12．求下列二元一次同余方程组的解：

(i) $3x+4y\equiv5 \pmod{13}$，$2x+5y\equiv7 \pmod{13}$；

(ii) $x+2y\equiv1 \pmod 5$，$2x+y\equiv1 \pmod 5$；

(iii) $x+3y\equiv1 \pmod 5$，$3x+4y\equiv2 \pmod 5$；

(iv) $4x+y\equiv2 \pmod 5$，$2x+3y\equiv1 \pmod 5$；

(v) $2x+3y\equiv5 \pmod 7$，$x+5y\equiv6 \pmod 7$；

(vi) $4x+y\equiv5 \pmod 7$，$x+2y\equiv4 \pmod 7$。

13．设$m\geqslant1$，$\Delta=ad-bc$，$(m,\Delta)=1$。那么，二元一次同余方程组

$$\begin{cases}ax+by\equiv e \pmod m,\\ cx+dy\equiv f \pmod m\end{cases}$$

对模 m 有唯一解：

$$x\equiv\Delta^{-1}(de-bf) \pmod m,\qquad y\equiv\Delta^{-1}(af-ce) \pmod m,$$

这里 $\Delta^{-1}\Delta\equiv1 \pmod m$。

14．设 $A=(a_{ij})$，$B=(b_{ij})$ ($1\leqslant i\leqslant n$，$1\leqslant j\leqslant l$) 是两个 n 行 l 列的整数矩阵，$m\geqslant1$。我们说矩阵 A 同余于矩阵 B 模 m，如果有 $a_{ij}\equiv b_{ij} \pmod m$，$1\leqslant i\leqslant n$，$1\leqslant j\leqslant l$，这时记作 $A\equiv B \pmod m$。这样，第13题中的二元一次同余方程组可表为

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\equiv\begin{pmatrix}e\\ f\end{pmatrix} \pmod m,$$

Δ就是矩阵$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$的行列式。当$(\Delta,m)=1$时，有唯一一组解：

$$\begin{pmatrix}x\\ y\end{pmatrix}\equiv\Delta^{-1}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}\begin{pmatrix}e\\ f\end{pmatrix} \pmod m.$$

15．设$A=(a_{ij})$是n阶整数矩阵，行列式$|A|=\Delta$，$(\Delta,m)=1$，

再设 $A^*=(a^*_{ij})$是A的伴随矩阵，即$a^*_{ij}=A_{ji}$，A_{ji}是矩阵A中元素a_{ji}的代数余子式（即矩阵A中除去第j行及第i列元素后，所得的$n-1$阶矩阵的行列式乘以$(-1)^{j+i}$）。证明：$\Delta^{-1}A^*A\equiv E(\bmod m)$，$E$是$n$阶单位矩阵（即在主对角线上的元素为1，其余元素均为零），$\Delta^{-1}\Delta\equiv 1(\bmod m)$。

16．在第15题的符号和条件下，n元一次同余方程组

$$A\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\equiv\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}(\bmod m)$$

对模m有唯一解：

$$\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\equiv\Delta^{-1}A^*\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}(\bmod m).$$

§4　一般同余方程的求解

在§2，§3中已完全解决了一次同余方程与一次同余方程组的求解问题，但是，对于高次同余方程，即使是二次同余方程也没有一般的求解方法，本节将介绍一种具体求解的一般算法。

我们以$T(m;f)$表示同余方程

$$f(x)\equiv 0(\bmod m)\tag{1}$$

的解数。

定理1　设$m=m_1\cdots m_k$，$m_1,\cdots,m_k$两两既约。那么，同余方程(1)与同余方程组

$$f(x)\equiv 0(\bmod m_j),\qquad 1\leqslant j\leqslant k\tag{2}$$

的解和解数相同，且有

$$T(m;f)=T(m_1;f)\cdots T(m_k;f).\tag{3}$$

证　由第三章§1性质Ⅸ知，同余方程(1)与同余方程组(2)的解（即满足两者的x的值）相同。设$t=T(m;f)$，$t_j=T(m_j;f)$

$(1\leqslant j\leqslant k)$。若(2)中的某个方程（不妨设是第 j_0 个方程）无解，则(1)必无解，这时 $t_{j_0}=0$，$t=0$，所以式(3)成立。现设 $t_j>0$ $(1\leqslant j\leqslant k)$，

$$x\equiv a_1^{(j)}, a_2^{(j)}, \cdots, a_{t_j}^{(j)} \pmod{m_j} \tag{4}$$

是(2)中第 j 个同余方程的全部解；

$$x\equiv a_1, a_2, \cdots, a_t \pmod{m} \tag{5}$$

是同余方程(1)的全部解。对每一个 $a_r(1\leqslant r\leqslant t)$，由于它是(2)中第 j 个同余方程的解，所以有且仅有一个 $a_{r_j}^{(j)}$ $(1\leqslant r_j\leqslant t_j)$ 满足

$$a_r\equiv a_{r_j}^{(j)} \pmod{m_j}. \tag{6}$$

这样，对每个 $a_r(1\leqslant r\leqslant t)$ 必有唯一的一组数

$$\{a_{r_1}^{(1)}, a_{r_2}^{(2)}, \cdots, a_{r_k}^{(k)}\} \tag{7}$$

与之对应。反过来，对由式(7)给出的每一组数，由§3定理1知，同余方程组

$$x\equiv a_{r_j}^{(j)} \pmod{m_j}, \qquad 1\leqslant j\leqslant k \tag{8}$$

必有唯一解

$$x\equiv c \pmod{m}.$$

显见，c 是同余方程组(2)的解，因而也是同余方程(1)的解，所以有且仅有一个 a_r 对所有的 $1\leqslant j\leqslant k$ 满足式(6)。因此，上面所说的对应是一一对应。因此有 $t=t_1\cdots t_k$，这就证明了解数相同，且有式(3)成立。证毕。

定理1实际上是给出了如何求解同余方程(1)的具体办法：即把模 m 分解为两两既约的较小模 m_j 的乘积，然后去求出每个同余方程 $f(x)\equiv 0 \pmod{m_j}$ 的全部解(4)，再对每一组数(7)（共有 $t_1\cdots t_k$ 组）去解一次同余方程组(8)，这样就求出了同余方程(1)的全部解。这个办法当然也可以用来求解同余方程组。通常，当 m 有素因数分解式

$$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

时，我们取 $m_j=p_j^{\alpha_j}$ $(1\leqslant j\leqslant k)$。这样，解一般合数模的同余方程(1) 就被归结为解模为素数幂的同余方程

$$f(x)\equiv 0(\bmod p^{\alpha}), \tag{9}$$

其中 p 为素数. 为了具体找这种同余方程的解，我们来指出这样一个简单的事实。

定理2 若同余方程 (1) 有解，则对任意的正整数 $d, d|m$，同余方程

$$f(x)\equiv 0(\bmod d) \tag{10}$$

也有解①。进而，若设

$$x\equiv c_1,\cdots,c_s(\bmod d) \tag{11}$$

是同余方程(10)的全部解，则对同余方程(1) 的每个解 a 有且仅有一个 c_i $(1\leqslant i\leqslant s)$ 满足

$$a\equiv c_i(\bmod d). \tag{12}$$

定理的证明十分简单，留给读者。这个定理告诉我们为了求较大模 m 的同余方程(1)的解，我们可以先找一个较小的 $d, d|m$，求出模 d 的同余方程(10) 的全部解(11)（当(10)无解则(1)当然也无解)，然后对每个 c_i 求同余方程(1)的形如

$$x=c_i+dy \tag{13}$$

的解，即解变数 y 的同余方程

$$g_i(y)\equiv f(c_i+dy)\equiv 0(\bmod m), \tag{14}$$

由此，就可求出(1)的全部解. 特别的，当 $m=p^{\alpha}$ 时，取 $d=p^{\alpha-1}$，同余方程(14)是一个一次同余方程（下面将证明这一点)，是一定可以解出的。因此，我们只要解出了模为素数 p 的同余方程——同余方程 (9)$(\alpha=1)$，就可以依次通过解一次同余方程，来解出模为 $p^2, p^3,\cdots$的同余方程——同余方程 (9)$(\alpha=2,3,\cdots)$。

定理3 设 p 是素数，整系数多项式

---

① 这就是§1定理 2。

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\qquad n\geqslant 2.\tag{15}$$

再设整数 $\alpha\geqslant 2$，c 是

$$f(x)\equiv 0 \pmod{p^{\alpha-1}}\tag{16}$$

的解. 那么，同余方程

$$f(x)\equiv 0 \pmod{p^{\alpha}}\tag{17}$$

的满足

$$x\equiv c \pmod{p^{\alpha-1}}\tag{18}$$

的解是

$$x\equiv c+y_jp^{\alpha-1} \pmod{p^{\alpha}},\qquad j=1,\cdots,l,\tag{19}$$

这里

$$y\equiv y_1,\cdots,y_l \pmod{p}\tag{20}$$

是一次同余方程

$$f'(c)y\equiv -f(c)p^{1-\alpha} \pmod{p}\tag{21}$$

的全部解，其中

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1.\tag{22}$$

证 这实际上是求由式（17），(18)给出的同余方程组的解。满足(18)的 x 必为

$$x=c+p^{\alpha-1}y.\tag{23}$$

把上式代入同余方程(17)，同余方程(17)变为

$$\begin{aligned}&a_n(c+p^{\alpha-1}y)^n+a_{n-1}(c+p^{\alpha-1}y)^{n-1}+\cdots\\&\quad+a_2(c+p^{\alpha-1}y)^2+a_1(c+p^{\alpha-1}y)+a_0\\&=f(c)+p^{\alpha-1}f'(c)y+A_2p^{2(\alpha-1)}y^2+\cdots+A_np^{n(\alpha-1)}y^n\\&\equiv 0 \pmod{p^{\alpha}},\end{aligned}\tag{24}$$

其中 $A_2,\cdots,A_n$ 是整数。由于 $\alpha\geqslant 2$，从上式知同余方程（17）变为 y 的一次同余方程

$$p^{\alpha-1}f'(c)y\equiv -f(c) \pmod{p^{\alpha}}.$$

由于 c 是同余方程（16）的解，所以 $p^{\alpha-1}\mid f(c)$. 因而，由第三章 §1性质Ⅳ知，上面的同余方程与同余方程（21)的解相同。这

样，利用式（23），（24）就可证明所要的结论：相应于同余方程（21）的全部解（20），式（19）给出了同余方程组（17）—（18）的不同的解，以及同余方程组（17）—（18）的每一个解一定可表为式（19）的形式，其中 y_j 为同余方程（21）的解。证毕。

由§2定理1、定理2及 p 是素数知，同余方程（21）的解可以出现三种情形：

（Ⅰ）$p\nmid f'(c)$。这时同余方程（21）的解数为1。所以，同余方程（17）满足条件（18）的解数为1，即 $l=1$。

（Ⅱ）$p|f'(c)$，$p\nmid f(c)p^{1-\alpha}$，即

$$f(c)\not\equiv 0 \pmod{p^{\alpha}},$$

这时同余方程（21）无解，所以同余方程（17）没有满足条件（18）的解，即 $l=0$。

（Ⅲ）$p|f'(c)$，$p|f(c)p^{1-\alpha}$，即

$$f(c)\equiv 0 \pmod{p^{\alpha}},$$

这时同余方程（21）的解数为 p，即

$$y\equiv 0,1,\cdots,p-1 \pmod{p}$$

均为（21）的解，所以同余方程（17）满足条件（18）的解数为 p，即 $l=p$。

由以上讨论立即可得到一个有用的结论：

推论4 在定理3的符号和条件下，若 c 是

$$f(x)\equiv 0 \pmod{p} \tag{25}$$

的解，且 $p\nmid f'(c)$。那么，对任意的 $\alpha\geqslant 2$，同余方程（17）满足条件（18）的解数均为1。特别当同余方程（25）与同余方程

$$f'(x)\equiv 0 \pmod{p}$$

无公共解时，同余方程（17）对任意的 $\alpha\geqslant 1$ 解数均相同。

详细证明留给读者。下面来举几个例子。

例1 解同余方程 $x^3+5x^2+9\equiv 0 \pmod{3^4}$。

解 同余方程

$$x^3+5x^2+9\equiv 0 \pmod{3}$$

有两个解：

$$x\equiv 0,1(\bmod 3).$$

现在 $f(x)=x^3+5x^2+9$，$f'(x)=3x^2+10x$，$f'(0)=0$，$f'(1)=13$。所以

$$3|f'(0),\quad 3\nmid f'(1).$$

进而解同余方程

$$x^3+5x^2+9\equiv 0(\bmod 3^2).$$

先求相应于 $x\equiv 0(\bmod 3)$ 的解。由于 $3|f'(0)$，及

$$f(0)=9\equiv 0(\bmod 3^2),$$

所以，

$$x\equiv -3,0,3(\bmod 3^2)$$

是解。再求相应于 $x\equiv 1(\bmod 3)$ 的解。由于 $3\nmid f'(1)$，相应的同余方程(21)是

$$13y\equiv -5(\bmod 3),$$

其解为 $y\equiv 1(\bmod 3)$，所以，得到解

$$x\equiv 4(\bmod 3^2).$$

进而解同余方程

$$x^3+5x^2+9\equiv 0(\bmod 3^3).$$

先求它相应于 $x\equiv -3,0,3(\bmod 3^2)$ 的解。由于

$$f(-3)=27,\qquad f(0)=9,\qquad f(3)=81,$$

所以，由（Ⅲ）知，相应于 $x\equiv -3(\bmod 3^2)$ 的解为

$$x\equiv -12,-3,6(\bmod 3^3);$$

相应于 $x\equiv 3(\bmod 3^2)$的解为

$$x\equiv -6,3,12(\bmod 3^3).$$

由（Ⅱ）知，没有相应于 $x\equiv 0(\bmod 3^2)$ 的解。再求相应于 $x\equiv 4(\bmod 3^2)$ 的解。这时，$f'(4)\equiv f'(1)\equiv 13\equiv 1\ (\bmod 3)$，$f(4)=153$，相应的同余方程（21）是

$$y\equiv -17\equiv 1(\bmod 3),$$

所以，得到解

$$x \equiv 13 (\bmod 3^3).$$

最后，解同余方程

$$x^3 + 5x^2 + 9 \equiv 0 (\bmod 3^4).$$

先求它相应于 $x \equiv -12, -3, 6 (\bmod 3^3)$ 的解。这时，

$$f(-12) = -999, \qquad f(-3) = 27, \qquad f(6) = 405.$$

所以，$3^4 \nmid f(-12)$，$3^4 \nmid f(-3)$，$3^4 \nmid f(6)$，因此由(II)和(III)知仅有相应于$f(6)$的解，再求相应于$x \equiv -6, 3, 12 (\bmod 3^3)$的解。这时

$$f(12) = 2457, \qquad f(3) = 81, \qquad f(-6) = -27,$$

因此，由（II）知没有相应于 $x \equiv -6, 12 (\bmod 3^3)$的解。由（III）知相应于$x \equiv -6; 3 (\bmod 3^3)$ 的解有

$$x \equiv -21, 6, 33; -24, 3, 30 (\bmod 3^4). \tag{26}$$

再求相应于 $x \equiv 13 (\bmod 3^3)$ 的解。由于 $f(13) = 3051$，所以相应的同余方程(21)是

$$y \equiv -113 \equiv 1 (\bmod 3).$$

相应的解是

$$x \equiv 40 (\bmod 3^4). \tag{27}$$

这样，式（26)，(27）就给出了所要求的全部解，解数为7。

例 2 解同余方程 $x^3 + 5x^2 + 9 \equiv 0 (\bmod 7 \cdot 3^4)$。

解 由定理 I 知，这就是要解同余方程组

$$\begin{cases} x^3 + 5x^2 + 9 \equiv 0 (\bmod 7), \\ x^3 + 5x^2 + 9 \equiv 0 (\bmod 3^4). \end{cases}$$

由直接计算知，第一个同余方程的解为

$$x \equiv -2 (\bmod 7).$$

由例 1 知第二个同余方程解为

$$x \equiv -21, 6, 33, -24, 3, 30, 40 (\bmod 3^4).$$

进而解一次同余方程组

$$\begin{cases} x \equiv a_1 (\bmod 7), \\ x \equiv a_2 (\bmod 3^4). \end{cases}$$

利用§3定理1，这里 $m_1=M_2=7$，$m_2=M_1=3^4$。由

$$M_1\equiv 9^2\equiv 2^2\equiv -3 \pmod 7$$

知，可取 $M_1^{-1}=2$。由

$$M_2\equiv 7 \pmod{3^4}$$

知，可取 $M_2^{-1}=-23$。因此，这个一次同余方程组的解是

$$\begin{aligned} x &\equiv 3^4\cdot 2\cdot a_1+7\cdot(-23)\cdot a_2 \\ &\equiv 162a_1-161a_2 \pmod{567}. \end{aligned}$$

分别用 $a_1=-2$，$a_2=-21,6,33,-24,3,30,40$ 代入就得到

$$x\equiv 3057,-1290,-5637,3540,-807,-5154,-6764 \pmod{567},$$

即

$$x\equiv 222,-156,33,138,-240,-51,40 \pmod{567}.$$

这就是所要求的同余方程的全部解，解数为7。

虽然定理3给出了模为素数幂的同余方程的一般解法，但有时是很麻烦的。把它和同余式的性质结合起来，往往能简化计算。

例3 解同余方程 $x^2+x+7\equiv 0 \pmod{3^3}$。

解 由§1恒等变形(Ⅲ)知，这同余方程的解与同余方程

$$4(x^2+x+7)\equiv 0 \pmod{3^3}$$

的解相同。这同余方程就是

$$(2x+1)^2+27\equiv(2x+1)^2\equiv 0 \pmod{3^3}.$$

显见，这同余方程的解（指 x 的值）与

$$2x+1\equiv 0 \pmod{3^2}$$

的解相同。直接计算知，解为

$$x\equiv 4 \pmod{3^2}.$$

所以，原同余方程的解是（为什么）

$$x\equiv -5,4,13 \pmod{3^3},$$

解数为3。

例4 求同余方程 $x^2\equiv 1 \pmod{2^l}$ 的解。

解 当 $l=1$ 时，解数为1，

$$x \equiv 1 \pmod 2.$$

当 $l=2$ 时，解数为2，

$$x \equiv -1, 1 \pmod{2^2}.$$

当 $l \geqslant 3$ 时，同余方程可写为

$$(x-1)(x+1) \equiv 0 \pmod{2^l}.$$

由于 x 是解时，必可表为 $x=2y+1$，代入上式得

$$4y(y+1) \equiv 0 \pmod{2^l},$$

即

$$y(y+1) \equiv 0 \pmod{2^{l-2}}.$$

所以必有

$$y \equiv 0, -1 \pmod{2^{l-2}}.$$

因此，解 x 必满足

$$x \equiv 1, -1 \pmod{2^{l-1}}.$$

所以原方程的解是（为什么）

$$x \equiv 1, 1+2^{l-1}, -1, -1+2^{l-1} \pmod{2^l},$$

解数为4.

例 5 设素数 $p>2$. 求同余方程 $x^2 \equiv 1 \pmod{p^l}$ 的解.

解 同余方程可写为

$$(x-1)(x+1) \equiv 0 \pmod{p^l}.$$

由于 $(x-1, x+1) \mid 2$，所以上式等价于

$$x-1 \equiv 0 \pmod{p^l} \quad 或 \quad x+1 \equiv 0 \pmod{p^l}.$$

因此，对任意的 $l \geqslant 1$ 解为

$$x \equiv -1, 1 \pmod{p^l},$$

解数为2.

例 6 解同余方程 $x^2 \equiv 2 \pmod{7^4}$.

解 模7^4的完全剩余系可表为

$$x = x_0 + x_1 \cdot 7 + x_2 \cdot 7^2 + x_3 \cdot 7^3,$$

$$-3 \leqslant x_j \leqslant 3, \qquad 0 \leqslant j \leqslant 3.$$

我们依次解同余方程

$$(x_0+x_1\cdot 7+\cdots+x_j\cdot 7^j)^2\equiv 2(\mathrm{mod}\ 7^{j+1}),\qquad 0\leqslant j\leqslant 3$$

来求出 x_0,x_1,x_2,x_3。当 $j=0$ 时，解

$$x_0^2\equiv 2(\mathrm{mod}\ 7),$$

得 $x_0=\pm 3$。当 $j=1$ 时，要解

$$(\pm 3+x_1 7)^2\equiv 2(\mathrm{mod}\ 7^2).$$

我们有

$$9\pm 6\cdot 7x_1\equiv 2(\mathrm{mod}\ 7^2),$$

$$\pm 6x_1\equiv -1(\mathrm{mod}\ 7),$$

得 $x_1=\pm 1$。当 $j=2$ 时，要求解

$$(\pm 3\pm 1\cdot 7+x_2 7^2)^2\equiv 2(\mathrm{mod}\ 7^3).$$

我们有

$$(\pm 3\pm 1\cdot 7)^2+2\cdot(\pm 3)\cdot 7^2x_2\equiv 2(\mathrm{mod}\ 7^3),$$

$$\pm 6x_2\equiv -2(\mathrm{mod}\ 7),$$

得 $x_2=\pm 2$。当 $j=3$ 时要解

$$(\pm 3\pm 1\cdot 7\pm 2\cdot 7^2+x_3\cdot 7^3)^2\equiv 2(\mathrm{mod} 7^4).$$

我们有

$$(\pm 3\pm 1\cdot 7\pm 2\cdot 7^2)^2\pm 6\cdot 7^3x_3\equiv 2(\mathrm{mod}\ 7^4),$$

$$100+40\cdot 7^2\pm 6\cdot 7^3x_3\equiv 2(\mathrm{mod}\ 7^4),$$

$$\pm 6\cdot 7x_3\equiv -2-40(\mathrm{mod}\ 7^2),$$

$$\pm 6x_3\equiv -6(\mathrm{mod}\ 7),$$

得 $x_3=\mp 1$。这样，同余方程有两个解：

$$x_1\equiv 3+1\cdot 7+2\cdot 7^2-7^3\equiv -235(\mathrm{mod}\ 7^4),$$

$$x_2\equiv -3-1\cdot 7-2\cdot 7^2+7^3\equiv 235(\mathrm{mod}\ 7^4).$$

例 6 的解法就是用整数的 k 进位表示来解模 k^l 的同余方程，k 不一定是素数。

习　题　四

1．求下列同余方程的解：

(i) $x^3+2x-3\equiv 0(\mathrm{mod}\ 45)$；

(ii) $4x^2-5x+13\equiv 0 \pmod{33}$；

(iii) $x^3-9x^2+23x-15\equiv 0 \pmod{143}$。

2．求下列模为素数幂的同余方程的解：

(i) $x^3+x^2+10x+1\equiv 0 \pmod{3^3}$；

(ii) $x^3+25x+3\equiv 0 \pmod{3^3}$；

(iii) $x^3-5x^2+3\equiv 0 \pmod{3^4}$；

(iv) $x^5+x^4+1\equiv 0 \pmod{3^4}$；

(v) $x^3-2x+4\equiv 0 \pmod{5^3}$；

(vi) $x^3+x+57\equiv 0 \pmod{5^3}$；

(vii) $x^3+x^2-4\equiv 0 \pmod{7^3}$；

(viii) $x^3+x^2-5\equiv 0 \pmod{7^3}$；

(ix) $x^2+5x+13\equiv 0 \pmod{3^3}$；

(x) $x^2+5x+13\equiv 0 \pmod{3^4}$；

(xi) $x^2\equiv 3 \pmod{11^3}$；　(xii) $x^2\equiv -2 \pmod{19^4}$。

3．求同余方程 $(x+1)^7-x^7-1\equiv 0 \pmod{7^7}$ 满足条件 $7\nmid x(1+x)$ 的解。

4．以 $T_1(m;f)$ 表示同余方程 $f(x)\equiv 0 \pmod{m}$ 满足条件 $(x,m)=1$ 的解数。证明：当 $(m_1,m_2)=1$ 时，$T_1(m_1m_2;f)=T_1(m_1;f)T_1(m_2;f)$。

5．设 $d\mid m$，整系数多项式 $f(x)$ 的每项系数均被 d 整除，$d\geqslant 1$。证明：$T(m;f)=dT(m/d;f/d)$，这里 $T(m;f)$ 表§4同余方程(1)的解数，f/d 表多项式 $f(x)/d$。

6．证明：(i) 同余方程组 $f(x)\equiv 0 \pmod{m}$，$x\equiv l \pmod{k}$ 有解的必要条件是 $(m,k)\mid f(l)$；

(ii) 以 $T(m,k,l;f)$ 表(i)中的同余方程组的解数，那么，当 $(m_1,m_2)=1$，且 m_1,m_2 均无大于1的平方因数时，

$$T(m_1m_2,k,l;f)=T(m_1,k,l;f)T(m_2,k,l;f)；$$

(iii) 以 $T_1(m,k,l;f)$ 表(i)中的同余方程组满足条件 $(x,m)=1$ 的解数。那么，在(ii)的条件下，

$$T_1(m_1 m_2,k,l;f)=T_1(m_1,k,l;f)\cdot T_1(m_2,k,l;f).$$

7．设 $m=2^{a_0}p_1^{a_1}\cdots p_r^{a_r}$，$p_j$ 是不同的奇素数，$a_j\geqslant 1(1\leqslant j\leqslant r)$，$a_0\geqslant 0$。证明：同余方程 $x^2\equiv 1(\bmod m)$ 的解数

$$T=\begin{cases}2^r, & a_0=0,1,\\ 2^{r+1}, & a_0=2,\\ 2^{r+2}, & a_0\geqslant 3.\end{cases}$$

8．把同余方程$x^2\equiv 1(\bmod m)$写为$(x-1)(x+1)\equiv 0(\bmod m)$。当$m$由上题给出时，利用把同余方程化为同余方程组的方法，提出一个求解 $x^2\equiv 1(\bmod m)$的全部解的具体方法。并用以求解$m=2^3\cdot 3^2\cdot 5^2, 2\cdot 3^2\cdot 5\cdot 7$ 的情形；

9．设 $m\geqslant 3$，T 由第 7 题给出。证明：

$$\prod_{r \bmod m}{}' r\equiv(-1)^{T/2}(\bmod m).$$

由此证明第三章 § 4 习题四第11题。

10．设 r 是m的不同素因子个数．证明：同余方程 $x^2\equiv x(\bmod m)$ 的解数为 2^r。

11．求同余方程 $x^2\equiv -1(\bmod m)$的解数（提示：利用第三章 §4习题四第 6 题，或利用本章 § 5的推论 3 ）。

12．(i) 设 $2\nmid a$，$2\nmid n$。证明：对任意 l，同余方程 $x^n\equiv a(\bmod 2^l)$ 恰有一解；

(ii) 设 p 为奇素数，$p\nmid a$，$p\nmid n$，证明对任意 l，同余方程 $x^n\equiv a(\bmod p^l)$ 的解数相同。

13．(i)用例 5 的方法继续解同余方程 $x^2\equiv 2(\bmod 7^l)$，$l=5,6,7$；

(ii) $x^2\equiv -1(\bmod 5^6)$；　　(iii)$x^2\equiv 4(\bmod 7^4)$。

14．设 $f(x)$是不等于常数的整系数多项式。证明：一定存在无穷多个素数 p，使同余方程 $f(x)\equiv 0(\bmod p)$ 有解。

15．设 $f(x)$是不等于常数的整系数多项式，r,s 为任给的

正整数。证明：一定存在整数 a，使得 $f(a)$，$f(a+1)$，…，$f(a+r-1)$ 中的每个数至少有 s 个不同的素因数。

§5 模为素数的二次同余方程

本节讨论模为素数的二次同余方程的一般理论，并在下两节讨论由此引出的 Legendre 符号，Gauss 二次互反律，以及 Jacobi 符号。由于 $p=2$ 的情形是显然的，下面恒假定 p 是奇素数。设 $p\nmid a$，二次同余方程的一般形式是

$$ax^2+bx+c\equiv 0(\bmod p). \tag{1}$$

由于 $p\nmid 4a$，所以(1)和同余方程

$$4a(ax^2+bx+c)\equiv 0(\bmod p)$$

的解相同，上式可写为

$$(2ax+b)^2\equiv b^2-4ac(\bmod p). \tag{2}$$

容易看出，通过变数替换①

$$y\equiv 2ax+b(\bmod p), \tag{3}$$

同余方程(2)与同余方程

$$y^2\equiv b^2-4ac(\bmod p) \tag{4}$$

是等价的。也就是说，两者同时有解或无解；有解时，对(4)的每个解 $y\equiv y_0(\bmod p)$，通过式(3)（这时是 x 的一次同余方程，$(p,2a)=1$，所以解数为 1）给出(2)的一个解 $x\equiv x_0(\bmod p)$，由(4)的不同的解给出(2)的不同的解，且反过来也对，此外两者解数相同。由以上讨论知，我们只要讨论形如

$$x^2\equiv d(\bmod p) \tag{5}$$

的同余方程。当 $p|d$ 时，(5)仅有一解

$$x\equiv 0(\bmod p),$$

所以，以后恒假定 $p\nmid d$。为了叙述方便，我们引进

① 由于是讨论模 p 的同余方程，变数替换 $y=2ax+b$ 和式(3)形式的模 p 的变数替换是一样的。

定义1 设素数 $p>2$，d 是整数，$p\nmid d$。如果同余方程 (5) 有解，则称 d 是模 p 的二次剩余；若无解，则称 d 是模 p 的二次非剩余。

例如，当 $p=3$ 时，$d\equiv1 \pmod 3$ 是模 3 的二次剩余，$d\equiv-1 \pmod 3$ 是模 3 的二次非剩余。当 $p=5$ 时，$d\equiv1, -1 \pmod 5$ 是模 5 的二次剩余，$d\equiv2, -2 \pmod 5$ 是模 5 的二次非剩余。当 $p=7$ 时，$d\equiv1,2,-3 \pmod 7$ 是模 7 的二次剩余，$d\equiv-1,-2,3 \pmod 7$ 是模 7 的二次非剩余。一般地有以下结论：

定理1 在模 p 的一个既约剩余系中，恰有 $(p-1)/2$ 个模 p 的二次剩余，$(p-1)/2$ 个模 p 的二次非剩余。此外，若 d 是模 p 的二次剩余，则同余方程(5)的解数为 2。

证 显见，只要取模 p 的绝对最小既约剩余系

$$-\frac{p-1}{2}, -\frac{p-1}{2}+1, \cdots, -1, 1, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2} \tag{6}$$

来讨论。d 是模 p 的二次剩余当且仅当

$$d\equiv\left(-\frac{p-1}{2}\right)^2, \left(-\frac{p-1}{2}+1\right)^2, \cdots, (-1)^2, 1^2, \cdots,$$

$$\left(\frac{p-1}{2}-1\right)^2, \left(\frac{p-1}{2}\right)^2 \pmod p.$$

由于 $(-j)^2\equiv j^2 \pmod p$，所以 d 是模 p 的二次剩余当且仅当

$$d\equiv1^2, \cdots, \left(\frac{p-1}{2}-1\right)^2, \left(\frac{p-1}{2}\right)^2 \pmod p. \tag{7}$$

当 $1\leqslant i<j\leqslant(p-1)/2$ 时，

$$i^2\not\equiv j^2 \pmod p, \tag{8}$$

所以，式(7)给出了模 p 的全部二次剩余，共有 $(p-1)/2$ 个。由于模 p 的既约剩余系有 $p-1$ 个数，所以另外的 $(p-1)/2$ 个必为模 p 的二次非剩余，这就证明了前一半结论。当 d 是模 p 的二次剩余时，由式(7)及(8)知，必有唯一的 i，$1\leqslant i\leqslant(p-1)/2$，使

$x \equiv i \pmod p$ 是(5)的解，进而就推出在既约剩余系(6)中有且仅有 $x \equiv \pm i \pmod p$ 是(5)的解，即(5)的解数为 2。证毕。

以后，为简单起见，我们就说模 p 有 $(p-1)/2$ 个二次剩余，$(p-1)/2$ 个二次非剩余。

例 1　求 $p = 11, 17, 19, 29$ 的二次剩余与二次非剩余。

j	1	2	3	4	5
$d \equiv j^2 \pmod{11}$	1	4	−2	5	3

模11的二次剩余是：1，−2，3，4，5；二次非剩余是：−1，2，−3，−4，−5。

j	1	2	3	4	5	6	7	8
$d \equiv j^2 \pmod{17}$	1	4	−8	−1	8	2	−2	−4

模17的二次剩余是：±1，±2，±4，±8；二次非剩余是 ±3，±5，±6，±7。

j	1	2	3	4	5	6	7	8	9
$d \equiv j^2 \pmod{19}$	1	4	9	−3	6	−2	−8	7	5

模19的二次剩余是：1，−2，−3，4，5，6，7，−8，9；二次非剩余是 −1，2，3，−4，−5，−6，−7，8，−9。

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$d \equiv j^2 \pmod{29}$	1	4	9	−13	−4	7	−9	6	−6	13	5	−1	−5	−7

模29的二次剩余是 ±1，±4，±5，±6，±7，±9，±13；二次非剩余是：±2，±3，±8，±10，±11，±12，±14。

由这些表不仅得到了模 p 的二次剩余 d，也可查出相应的二次同余方程(5)的两个解 $\pm j \pmod p$。例如，−2是模19的二次剩

余，$x^2 \equiv -2 \pmod{19}$的两个解是 $\pm 6 \pmod{19}$。

下面的定理从理论上给出了判别 d 是否是模 p 的二次剩余的方法。通常称为 Euler 判别法。

定理2 设素数 $p>2$，$p \nmid d$。那么，d 是模 p 的二次剩余的充要条件是

$$d^{(p-1)/2} \equiv 1 \pmod{p}; \tag{9}$$

d 是模 p 的二次非剩余的充要条件是

$$d^{(p-1)/2} \equiv -1 \pmod{p}. \tag{10}$$

证 首先来证明对任一$d, p \nmid d$，式(9) 或(10)有且仅有一式成立。由第三章 § 3 定理 3 知

$$d^{p-1} \equiv 1 \pmod{p},$$

因而有

$$(d^{(p-1)/2}-1)(d^{(p-1)/2}+1) \equiv 0 \pmod{p}. \tag{11}$$

由于素数 $p>2$ 及

$$(d^{(p-1)/2}-1, d^{(p-1)/2}+1) \mid 2,$$

所以，由式(11)立即推出式(9)或式(10)有且仅有一式成立。

下面来证明 d 是模 p 的二次剩余的充要条件是式(9) 成立。先证必要性。若 d 是模 p 的二次剩余，则必有 x_0使得

$$x_0^2 \equiv d \pmod{p},$$

因而有

$$x_0^{p-1} \equiv d^{(p-1)/2} \pmod{p}.$$

由于 $p \nmid d$，所以 $p \nmid x_0$，因此由第三章 § 3 定理 3 知

$$x_0^{p-1} \equiv 1 \pmod{p}.$$

由以上两式就推出式(9) 成立。再证充分性。证明的方法与第三章 § 4定理 1 的证法一样。设式(9) 成立，这时必有 $p \nmid d$。考虑一次同余方程

$$ax \equiv d \pmod{p}. \tag{12}$$

由 § 2定理 1 及 $p \nmid d$ 知，对由式(6) 给出的模 p 的既约剩余系中的每个 j，当 $a=j$ 时，必有唯一的 $x=x_j$ 属于既约剩余系(6)，

使得式(12)成立。若 d 不是模 p 的二次剩余，则必有 $j\neq x_j$。这样，既约剩余系(6)中的 $p-1$ 个数就可按 j, x_j 作为一对，两两分完。由此及第三章§4定理1知

$$-1\equiv(p-1)!\equiv(-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv d^{(p-1)/2}(\bmod p).$$

(13)

但这和式(9)矛盾。所以必有某一 j_0，使 $j_0=x_{j_0}$，由此及式(12)知 d 是模 p 的二次剩余。这就证明了充分性。

由已经证明的这两部分结论，立即推出定理剩下的结论（为什么）.证毕。

由定理2立即推出两个有用的结论。

推论3① -1 是模 p 的二次剩余的充要条件是 $p\equiv1(\bmod 4)$；当 $p\equiv1(\bmod 4)$时，

$$\left(\pm\left(\frac{p-1}{2}\right)!\right)^2\equiv-1(\bmod p). \tag{14}$$

证 由定理2知，-1 是模 p 的二次剩余的充要条件是

$$(-1)^{(p-1)/2}\equiv1(\bmod p).$$

由此及 $p>2$ 推出充要条件是

$$(-1)^{(p-1)/2}=1,$$

即 $p\equiv1(\bmod 4)$。当 $p\equiv1(\bmod 4)$ 时，由式(13)的第一个同余关系式就推出式(14)成立。

推论4 设素数 $p>2$，$p\nmid d_1$，$p\nmid d_2$。那么，

(i) 若 d_1,d_2 均为模 p 的二次剩余，则 d_1d_2 也是模 p 的二次剩余；

(ii) 若 d_1,d_2 均为模 p 的二次非剩余，则 d_1d_2 是模 p 的二次剩余；

(iii) 若 d_1 是模 p 的二次剩余，d_2 是模 p 的二次非剩余，则

① 推论3就是第三章§4习题四的第6题及第4题(ii)。

$d_1 d_2$ 是模 p 的二次非剩余。

这由定理 2 及

$$(d_1 d_2)^{(p-1)/2} = d_1^{(p-1)/2} \cdot d_2^{(p-1)/2}$$

立即推出。

定理 2 并不是一个实用的判别法，因为对具体的素数 p，当它不太大时，我们可以通过直接计算式(6) 的下面的式子来直接确定哪些 d 是二次剩余，哪些是二次非剩余。这比验证同余式(9) 要简单。当 p 较大时，这两种办法都不实用。另外一个问题是给定了 d，问怎样的 p 以 d 为它的二次剩余。例如推论 3 就解决了 $d=-1$ 这一最简单的情形。下节将讨论这两个问题。

例 2 利用定理 2 来判断：

(i) 3 是不是模 17 的二次剩余；

(ii) 7 是不是模 29 的二次剩余。

解 由 $3^3 \equiv 10 \pmod{17}$，$3^4 \equiv 30 \equiv -4 \pmod{17}$，$3^8 \equiv -1 \pmod{17}$ 知，3 是模17的二次非剩余。

由 $7^2 \equiv -9 \pmod{29}$，$7^3 \equiv -5 \pmod{29}$，$7^6 \equiv -4 \pmod{29}$，$7^7 \equiv 1 \pmod{29}$，$7^{14} \equiv 1 \pmod{29}$ 知，7 是模 29 的二次剩余。

例 3 判断下列同余方程的解数：

(i) $x^2 \equiv -1 \pmod{61}$；　　(ii) $x^2 \equiv 16 \pmod{51}$；

(iii) $x^2 \equiv -2 \pmod{209}$；　　(iv) $x^2 \equiv -63 \pmod{187}$。

解 由推论 3 知方程(i)的解数为 2。同余方程(ii)等价于方程组：$x^2 \equiv 1 \pmod 3$，$x^2 \equiv -1 \pmod{17}$。这两个方程解数均为2，由 §4 定理 1 知，同余方程(ii)的解数为 4。同余方程(iii) 等价于方程组：$x^2 \equiv -2 \pmod{11}$，$x^2 \equiv -2 \pmod{19}$，由例1的表知，这两个方程解数均为 2，由 §4 定理 1 知，同余方程(iii)的解数为 4。同余方程(iv)等价于方程组 $x^2 \equiv 3 \pmod{11}$，$x^2 \equiv 5 \pmod{17}$，由例 1 的表知，后一方程无解，所以原方程无解。

习 题 五

1．求模 $p=13,23,37,41$ 的二次剩余，二次非剩余．

2．在不超过 100 的素数 p 中，2 是哪些模 p 的二次剩余？-2 是哪些模 p 的二次剩余？

3．利用定理 2 判断：

(i) -8 是不是模 53 的二次剩余；

(ii) 8 是不是模 67 的二次剩余．

4．求下列同余方程的解数：

(i) $x^2\equiv -2 \pmod{67}$；　　(ii) $x^2\equiv 2 \pmod{67}$；

(iii) $x^2\equiv -2 \pmod{37}$；　　(iv) $x^2\equiv 2 \pmod{37}$；

(v) $x^2\equiv -1 \pmod{221}$；　　(vi) $x^2\equiv -1 \pmod{427}$；

(vii) $x^2\equiv -2 \pmod{209}$；　　(viii) $x^2\equiv 2 \pmod{391}$；

(ix) $x^2\equiv 4 \pmod{45}$；　　(x) $x^2\equiv 5 \pmod{539}$．

5．设 p 是奇素数，$p\nmid a$．证明：存在整数 $u,v,(u,v)=1$，使得 $u^2+av^2\equiv 0 \pmod{p}$ 的充要条件是 $-a$ 是模 p 的二次剩余．

6．设 p 是奇素数．把 $1,2,\cdots,p-1$ 分为两个集合 S_1,S_2，满足以下条件：(i) S_1,S_2 均非空集；(ii) 属于同一个集合中的两数相乘之积必和 S_1 中的某个数同余于模 p；(iii) 属于不同集合的两数之积必和 S_2 中的某个数同余于模 p．证明：S_1 由 $1,2,\cdots,p-1$ 中所有的模 p 的二次剩余组成；S_2 由其中的所有模 p 的二次非剩余组成，且各有 $(p-1)/2$ 个数．

7．设 p 是奇素数．证明：

(i) 模 p 的所有二次剩余的乘积对模 p 的剩余是

$$(-1)^{(p+1)/2};$$

(ii) 模 p 的所有二次非剩余的乘积对模 p 的剩余是

$$(-1)^{(p-1)/2};$$

(iii) 模 p 的所有二次剩余之和对模 p 的剩余是：1，当 $p=3$；0，当 $p>3$；

(iv) 所有二次非剩余之和对模 p 的剩余是多少？

8. 设 p 是素数。$(a,p)=(b,p)=1$。证明：若 $x^2\equiv a \pmod p$ 与 $x^2\equiv b \pmod p$ 均无解，则 $x^2\equiv ab \pmod p$ 有解。

9. 设 $(a,m)=1$。若 $x^2\equiv a \pmod m$ 有解则称 a 是模 m 的二次剩余。证明：

(i) 当 $m>2$ 时，a 是模 m 的二次剩余的必要条件是 $a^{\phi(m)/2}\equiv 1 \pmod m$。这条件充分吗？举例说明。

(ii) 若 a 是模 m 的二次剩余，$ab\equiv 1 \pmod m$，则 b 也是模 m 的二次剩余；

(iii) 利用(ii)证明第 7 题的(i)和(ii)；

(iv) 对合数模 m，§ 5 定理 1 成立吗？以 $m=12,15,22,25,28$ 为例，列表说明；

(v) 对合数模 m 来说，两个二次非剩余之积一定是二次剩余吗？

(vi) 模 m 的二次剩余有 $\phi(m)/T$ 个，T 由 § 4 习题四第 7 题给出。

10. 设 p 是奇素数 $\equiv 1 \pmod 4$。证明：

(i) $1,2,\cdots(p-1)/2$ 中模 p 的二次剩余与二次非剩余的个数均为 $(p-1)/4$ 个；

(ii) $1,2,\cdots,p-1$ 中有 $(p-1)/4$ 个偶数为模 p 的二次剩余，$(p-1)/4$ 个奇数为模 p 的二次剩余；

(iii) $1,2,\cdots,p-1$ 中有 $(p-1)/4$ 个偶数为模 p 的二次非剩余、$(p-1)/4$ 个奇数为模 p 的二次非剩余；

(iv) $1,2,\cdots,p-1$ 中全体模 p 的二次剩余之和等于

$$p(p-1)/4;$$

(v) $1,2,\cdots,p-1$ 中全体模 p 的二次非剩余之和等于

$$p(p-1)/4.$$

11. 设 p 是奇素数。证明：$1,2,\cdots,p-1$ 中全体模 p 的二次剩余之和

$$S = p(p^2 - 1)/24 - p\sum_{j=1}^{(p-1)/2}\left[\frac{j^2}{p}\right].$$

由此推出，当 $p\equiv 1 \pmod 4$ 时，

$$p\sum_{j=1}^{(p-1)/2}\left[\frac{j^2}{p}\right] = \frac{p(p^2-1)}{24} - \frac{p(p-1)}{4}.$$

以 $p = 3,5,7,11,13,17,19,23,29,31,37$ 来具体验证所得公式的正确性.

12. (i) 证明：当 $0\leqslant\{x\}<1/2$ 时，$\{2x\}-\{x\}=\{x\}$；当 $1/2\leqslant\{x\}<1$ 时，$\{2x\}-\{x\}=\{x\}-1$；

(ii) 设 $1\leqslant j<(p-1)/2$，p 是奇素数. 利用

$$j^2 = p\left(\left[\frac{2j^2}{p}\right]-\left[\frac{j^2}{p}\right]\right)+p\left(\left\{\frac{2j^2}{p}\right\}-\left\{\frac{j^2}{p}\right\}\right),$$

证明：j^2 对模 p 的绝对最小剩余为正的充要条件是 $\{j^2/p\}<1/2$，即 $[2j^2/p]-2[j^2/p]=0$；j^2 对模 p 的绝对最小剩余为负的充要条件是 $\{j^2/p\}>1/2$，即 $[2j^2/p]-2[j^2/p]=1$；

(iii) 在 $1,2,\cdots,(p-1)/2$ 中模 p 的二次非剩余个数等于

$$N_1 = \sum_{j=1}^{(p-1)/2}\left(\left[\frac{2j^2}{p}\right]-2\left[\frac{j^2}{p}\right]\right);$$

(iv) 当 $p\equiv 1 \pmod 4$ 时，

$$\sum_{j=1}^{(p-1)/2}\left(\left[\frac{2j^2}{p}\right]-2\left[\frac{j^2}{p}\right]\right)=\frac{p-1}{4}.$$

(v) 以 $p=3,5,7,11,13,17,19,23,29,31,37$ 来具体验证上述结论的正确性并比较在 $1,2,\cdots,(p-1)/2$ 中模 p 的二次剩余与非剩余的个数的多少.

13. 设 $m>1$，$(a,m)=1$. 证明：二元一次同余方程

$$ax + y \equiv 0 \pmod m$$

一定有一组解 $x = x_0, y = y_0$，满足 $0<|x_0|\leqslant\sqrt{m}$，$0<|y_0|\leqslant\sqrt{m}$

（提示：利用鸽巢原理）。

14．把上题的结论进一步改进为 x_0, y_0 满足：$0<|x_0|\leqslant\sqrt{m}$，$0<|y_0|<\sqrt{m}$。

15．设 $m>1, (a, m)=1$。再设正整数 e，f 满足：$ef>m$，$e>1, f>1$。证明：二元一次同余方程 $ax+y\equiv0 \pmod m$ 一定有一组解 $x=x_0, y=y_0$，满足：$0<|x_0|<e, 0<|y_0|<f$。

16．设素数 $p\equiv1 \pmod 8$，证明：必有奇素数 $q, 0<q<\sqrt{p}$，是模 p 的二次非剩余（提示：任取一个模 p 的二次非剩余 a，考虑二元一次同余方程 $ax+y\equiv0 \pmod p$）。

17．设素数 $p>2, (p, d)=1$，a 是同余方程 $u^2+d\equiv0 \pmod p$ 的解。证明：

(i) $ax+y\equiv0 \pmod p$ 的任一组解 $x=x_0, y=y_0$，一定是 $dx^2+y^2\equiv0 \pmod p$ 的一组解；

(ii) $dx^2+y^2\equiv0 \pmod p$ 的任一组解 $x=x_0, y=y_0$，一定是 $ax+y\equiv0 \pmod p$ 或 $ax-y\equiv0 \pmod p$ 的一组解。

§6 Legendre 符号，Gauss 二次互反律

为了便于讨论，我们引进一个表示模 p 的二次剩余、二次非剩余的符号——Legendre 符号。

定义1 设素数 $p>2$。定义整变数 d 的函数

$$\left(\frac{d}{p}\right)=\begin{cases} 1, & \text{当 } d \text{ 是模 } p \text{ 的二次剩余；} \\ -1, & \text{当 } d \text{ 是模 } p \text{ 的二次非剩余；} \\ 0, & \text{当 } p\mid d\text{。} \end{cases}$$

我们把 $\left(\frac{d}{p}\right)$ 称为是模 p 的 Legendre 符号。

利用引进的 Legendre 符号，上节的定理 2，推论 4 可表述为 Legendre符号的性质。

定理1 Legendre 符号有以下性质：

(i) $\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right)$;

(ii) $\left(\frac{d}{p}\right)\equiv d^{(p-1)/2}(\bmod p)$;

(iii) $\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{c}{p}\right)$;

(iv) 当 $p\nmid d$ 时，$\left(\frac{d^2}{p}\right)=1$;

(v) $\left(\frac{1}{p}\right)=1$，$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$.

证明是十分简单的，留给读者。

这样，确定 d 是否是模 p 的二次剩余就变为去计算 Legendre 符号$\left(\frac{d}{p}\right)$的值。定理 1 的性质可以用来计算$\left(\frac{d}{p}\right)$，并由算术基本定理知，只要能计算出

$$\left(\frac{-1}{p}\right),\quad \left(\frac{2}{p}\right),\quad \left(\frac{q}{p}\right),$$

就可以计算出任意的$\left(\frac{d}{p}\right)$，这里 $q>2$ 是小于 p 的素数。解决这些问题的基础是下面的 Gauss 引理。

引理2 设素数 $p>2$，$p\nmid d$。再设 $1\leqslant j<p/2$,

$$t_j\equiv jd(\bmod p),\quad 0<t_j<p. \tag{1}$$

以 n 表示这 $(p-1)/2$ 个 $t_j(1\leqslant j<p/2)$ 中大于 $p/2$ 的 t_j 的个数。那么，有

$$\left(\frac{d}{p}\right)=(-1)^n.$$

证 对任意的 $1\leqslant j<i<p/2$,

$$t_j\pm t_i\equiv(j\pm i)d\not\equiv 0(\bmod p),$$

即

$$t_j\not\equiv\pm t_i(\bmod p). \tag{2}$$

我们以 $r_1,\cdots,r_n$ 表 $t_j(1\leqslant j<p/2)$ 中所有大于 $p/2$ 的数，以 $s_1,\cdots,s_k$ 表 $t_j(1\leqslant j<p/2)$ 中所有小于 $p/2$ 的数。显然有

$$1\leqslant p-r_i<p/2.$$

由式(2) 知

$$s_j\not\equiv p-r_i\pmod p,\quad 1\leqslant j\leqslant k,\ 1\leqslant i\leqslant n.$$

因此，$s_1,\cdots,s_k,p-r_1,\cdots,p-r_n$ 这 $(p-1)/2$ 个数恰好就是 $1,2,\cdots,(p-1)/2$ 的一个排列。由此及式(1)得

$$\begin{aligned}1\cdot 2\cdot\cdots\cdot(p-1)/2\cdot d^{(p-1)/2}&\equiv t_1t_2\cdots t_{(p-1)/2}\\ &\equiv s_1\cdots s_k\cdot r_1\cdots r_n\\ &\equiv(-1)^n s_1\cdots s_k\cdot(p-r_1)\cdots(p-r_n)\\ &\equiv(-1)^n\cdot 1\cdot 2\cdots(p-1)/2\pmod p.\end{aligned}$$

进而有

$$d^{(p-1)/2}\equiv(-1)^n\pmod p,$$

由此及定理 1 (ii)，定义 1 就推出所要结论。

由引理 2 就可推出

定理3 我们有

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}.$$

证 利用引理 2 中的符号，取 $d=2$。容易看出，

$$\begin{aligned}&1\leqslant t_j=2j<p/2,\quad 1\leqslant j<p/4,\\ &p/2<t_j=2j<p,\quad p/4<j<p/2.\end{aligned}$$

由第二式知

$$n=\frac{p-1}{2}-\left[\frac{p}{4}\right].$$

因而有

$$n=\begin{cases}l, & p=4l+1,\\ l+1, & p=4l+3.\end{cases}$$

由此及引理 2 就得到

$$\left(\frac{2}{p}\right)=(-1)^n=\begin{cases}1, & p\equiv\pm1\pmod 8,\\ -1, & p\equiv\pm3\pmod 8.\end{cases}\tag{3}$$

这就是所要证明的结论。式(3)表明当且仅当素数 $p\equiv\pm1\pmod 8$ 时，2才是模 p 的二次剩余。

下面来对引理2及其证明作进一步分析。利用符号整数部分 $[x]$，式(1)可表为

$$jd=p\left[\frac{jd}{p}\right]+t_j,\quad 1\leqslant j<p/2.$$

两边对 j 求和得

$$d\sum_{j=1}^{(p-1)/2}j=p\sum_{j=1}^{(p-1)/2}\left[\frac{jd}{p}\right]+\sum_{j=1}^{(p-1)/2}t_j=pT+\sum_{j=1}^{(p-1)/2}t_j.$$

由引理2的证明知

$$\begin{aligned}\sum_{j=1}^{(p-1)/2}t_j&=s_1+\cdots+s_k+r_1+\cdots+r_n\\&=s_1+\cdots+s_k+(p-r_1)+\cdots+(p-r_n)-np+2(r_1+\cdots+r_n)\\&=\sum_{j=1}^{(p-1)/2}j-np+2(r_1+\cdots+r_n).\end{aligned}$$

由以上两式得

$$\frac{p^2-1}{8}(d-1)=p(T-n)+2(r_1+\cdots+r_n).\tag{4}$$

从式(4)立即推出：

定理4 设素数 $p>2$。当 $(d,2p)=1$ 时，

$$\left(\frac{d}{p}\right)=(-1)^T,\tag{5}$$

其中

$$T=\sum_{j=1}^{(p-1)/2}\left[\frac{jd}{p}\right];\tag{6}$$

以及定理 3 成立。

证 当$(d,2p)=1$时，由式(4)得

$$T-n\equiv 0 \pmod 2.$$

由此及引理 2 即得式(4)。当 $d=2$时，显然有 $T=0$，所以由式(4)得

$$n\equiv\frac{p^2-1}{8} \pmod 2.$$

由此及引理 2 就推出定理 3（这给出了定理 3 的又一证明）。

当 d 为正数时，定理 4 中的T有十分明确几何意义：T 表示直角坐标平面中由 x 轴、直线 $x=p/2$及直线 $y=dx/p$ 所围成的三角形 OAB 内部的整点个数①（见图 1）。这只要注意到：在线

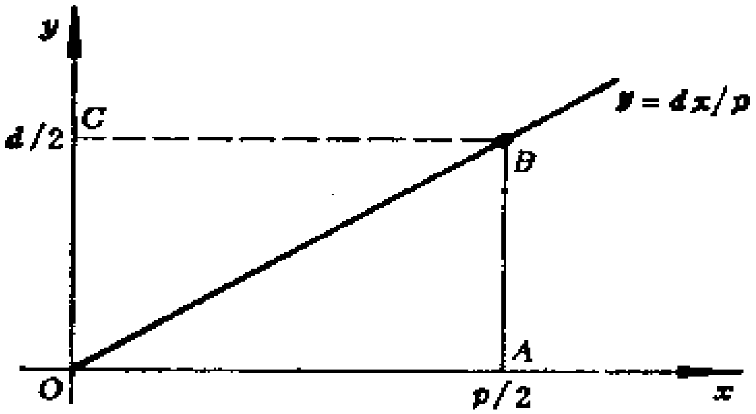


图 1

段 AB 和线段OB上均无整点(除了原点)，后者是因为 $(p,d)=1$。如果 d 也是奇素数，设$d=q\neq p$，那末，同样有

$$\left(\frac{p}{q}\right)=(-1)^S, \tag{7}$$

其中

$$S=\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right].$$

① 整点即是坐标均为整数的点，参看第一章 § 8例1。

同样地，S 就是图 1 中的三角形 OCB 内部的整点个数（取 $d=q$）。这样一来，$S+T$ 就是矩形 $OABC$ 内部的整点数，所以有

$$S+T=\frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{8}$$

由式(5)（取 $d=q$），(7)及(8)就证明了著名的Gauss二次互反律：

定理5 设 p,q 均为奇素数，$p\neq q$。那末有

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{(p-1)/2\cdot(q-1)/2}. \tag{9}$$

定理 5 表明：两个奇素数 p,q，只要有一个数 $\equiv 1 \pmod 4$，就必有

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right);$$

当且仅当它们都是 $4k+3$ 形式的数时，才有

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right).$$

由 Legendre 符号定义知，$\left(\frac{q}{p}\right)$和$\left(\frac{p}{q}\right)$分别刻画了二次同余方程

$$x^2\equiv q \pmod p$$

和

$$x^2\equiv p \pmod q$$

是否有解，即 q 是否是模 p 的二次剩余和 p 是否是模 q 的二次剩余，这里正好是模和剩余互换了位置。定理 5 就是刻画了这两者之间的关系，所以称为二次互反律。二次互反律是初等数论中最重要的基本定理之一。它不仅可用来计算 Legendre 符号（结合定理 1 和 3），而且它有重要的理论价值。下面来举几个例子。

例 1 计算 $\left(\frac{137}{227}\right)$.

解　227是素数，由定理1得

$$\left(\frac{137}{227}\right)=\left(\frac{-90}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2\cdot3^2\cdot5}{227}\right)$$

$$=(-1)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right)$$

$$=(-1)\left(\frac{2}{227}\right)\left(\frac{5}{227}\right).$$

由定理3得

$$\left(\frac{2}{227}\right)=-1.$$

由定理5，定理1及定理3得

$$\left(\frac{5}{227}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

由以上三式得

$$\left(\frac{137}{227}\right)=-1.$$

这表明同余方程 $x^2\equiv137 \pmod{227}$ 无解。

例2　判断同余方程

(i) $x^2\equiv-1 \pmod{365}$；　　(ii) $x^2\equiv2 \pmod{3599}$

是否有解，有解时求出其解数。

解　(i) 365不是素数，$365=5\cdot73$。所以同余方程和同余方程组

$$x^2\equiv-1 \pmod 5,\quad x^2\equiv-1 \pmod{73}$$

等价。由定理1(v)知

$$\left(\frac{-1}{5}\right)=\left(\frac{-1}{73}\right)=1,$$

所以，同余方程组有解。由§4定理1及§5定理1知，原同余方

程有解，解数为4。

(ii) 3599不是素数，3599 = 59·61. 同余方程等价于同余方程组

$$x^2 \equiv 2 \pmod{59}, \quad x^2 \equiv 2 \pmod{61}.$$

由定理3知$\left(\frac{2}{59}\right) = -1$，所以无解。

例3 求所有奇素数p，它以3为其二次剩余。

解 这就是要求所有奇素数p使$\left(\frac{3}{p}\right)=1$. 由定理5知

$$\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

显见，p是大于3的奇素数. 由

$$(-1)^{(p-1)/2}=\begin{cases} 1, & p\equiv 1 \pmod 4, \\ -1, & p\equiv -1 \pmod 4 \end{cases}$$

及

$$\left(\frac{p}{3}\right)=\begin{cases} \left(\frac{1}{3}\right)=1, & p\equiv 1 \pmod 6, \\ \left(\frac{-1}{3}\right)=-1, & p\equiv -1 \pmod 6 \end{cases}$$

知，$\left(\frac{3}{p}\right)=1$的充要条件是

$$p\equiv 1 \pmod 4, \quad p\equiv 1 \pmod 6; \tag{10}$$

或

$$p\equiv -1 \pmod 4, \quad p\equiv -1 \pmod 6. \tag{11}$$

由同余方程组(10)知，$p\equiv 1 \pmod{12}$，由(11)知，$p\equiv -1 \pmod{12}$. 因此，3是模p的二次剩余的充要条件是$p\equiv \pm 1 \pmod{12}$. 由此推出3是模p的二次非剩余的充要条件是$p\equiv \pm 5 \pmod{12}$（为什么）。

对3这样小的数仍然可以直接用引理2，如同定理3那样来

解例3．利用引理2的符号，取 $d=3$。我们有

$$1\leqslant t_j=3j<p/2,\quad 1\leqslant j<p/6,$$
$$p/2<t_j=3j<p,\quad p/6<j<p/3,$$
$$p<t_j=3j<3p/2,\quad p/3<j<p/2,$$

从最后一式得

$$0<t_j-p<p/2,\quad p/3<j<p/2.$$

注意到 $p>3$，从以上讨论知

$$n=[p/3]-[p/6].$$

因此，

$$n=\begin{cases}\left[\dfrac{6k+1}{3}\right]-\left[\dfrac{6k+1}{6}\right]=k, & p=6k+1,\\[2ex] \left[\dfrac{6k-1}{3}\right]-\left[\dfrac{6k-1}{6}\right]=k, & p=6k-1.\end{cases}$$

所以有

$$\left(\frac{3}{p}\right)=\begin{cases}1, & p\equiv\pm1\pmod{12},\\ -1, & p\equiv\pm5\pmod{12}.\end{cases}$$

这得到了和上面同样的结果。但对大的数用二次互反律来做比较方便，不易出错。

例4 求以11为其二次剩余的所有奇素数 p。

解 由定理5知

$$\left(\frac{11}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{11}\right).$$

由直接计算知

$$\left(\frac{p}{11}\right)=\begin{cases}1, & p\equiv1,-2,3,4,5\pmod{11},\\ -1, & p\equiv-1,2,-3,-4,-5\pmod{11}.\end{cases}$$

$$(-1)^{(p-1)/2}=\begin{cases}1, & p\equiv1\pmod4,\\ -1, & p\equiv-1\pmod4.\end{cases}$$

解同余方程组

$$\begin{cases} x \equiv a_1 \pmod 4, \\ x \equiv a_2 \pmod{11} \end{cases}$$

可得（留给读者）：

$$x \equiv -11a_1 + 12a_2 \pmod{44}.$$

综合以上讨论知，$\left(\frac{11}{p}\right)=1$ 当且仅当

$$p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}. \qquad (12)$$

所以当 p 为以上形式的素数时，11为其二次剩余．进而推出当 $p \neq 11$ 为以下形式的素数时，$\left(\frac{11}{p}\right)=-1$，即11为模 p 的二次非剩余：

$$p \equiv \pm 3, \pm 21, \pm 13, \pm 15, \pm 17 \pmod{44}. \qquad (13)$$

例 5 证明：若 $\left(\frac{d}{p}\right)=-1$，则 p 一定不能表为 x^2-dy^2 的形式。

证 用反证法．若 $p=x^2-dy^2$，因 p 是素数，故必有 $(p,x)=(p,y)=1$．因而由定理 1 推出

$$1=\left(\frac{x^2}{p}\right)=\left(\frac{dy^2}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{y^2}{p}\right)=\left(\frac{d}{p}\right).$$

矛盾．这样，由例 3 知，当 $p \equiv \pm 5 \pmod{12}$ 时一定不能表为 x^2-3y^2 的形式．由例 3 可得

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\begin{cases} 1, & p \equiv 1, -5 \pmod{12}, \\ -1, & p \equiv -1, 5 \pmod{12}. \end{cases} \qquad (14)$$

因此，当 $p \equiv -1, 5 \pmod{12}$ 时一定不能表为 x^2+3y^2 的形式．进而推出，当 $p \equiv 5 \pmod{12}$ 时一定不能表为 $x^2 \pm 3y^2$ 的形式

例 6 证明：有无穷多个素数 $p \equiv 1 \pmod 4$．

证 假设这样的素数只有有限个，设为 $p_1, \cdots, p_k$．考虑 $(2p_1 \cdots p_k)^2+1=P$．由假设及 $P \equiv 1 \pmod 4$ 知，P 不是素数．设 p

是P的素因数，p当然是奇数，所以-1是模p的二次剩余，即$\left(\frac{-1}{p}\right)=1$。由定理1知$p\equiv1(\bmod 4)$，但显然有$p\neq p_j(1\leqslant j\leqslant k)$，这和假设矛盾。证毕。

例7 证明：x^4+1的奇素因数$p\equiv1(\bmod 8)$。进而推出有无穷多个素数$p\equiv1(\bmod 8)$。

证 设p是x^4+1的奇素因数，即

$$(x^2)^2\equiv x^4\equiv-1(\bmod p),$$

因而有$\left(\frac{-1}{p}\right)=1$。由定理1知$p\equiv1(\bmod 4)$。而另一方面

$$x^4+1=(x^2+1)^2-2x^2,$$

所以有

$$(x^2+1)^2\equiv2x^2(\bmod p)。$$

由于$(p,2x)=1$，所以有（利用定理1）

$$1=\left(\frac{(x^2+1)^2}{p}\right)=\left(\frac{2x^2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{x^2}{p}\right)=\left(\frac{2}{p}\right).$$

由此从定理3推出$p\equiv\pm1(\bmod 8)$。因而必有$p\equiv1(\bmod 8)$。

下面来证明第二个结论。若这样的素数只有有限个，设为$p_1,\cdots,p_k$。考虑$P=(2p_1\cdots p_k)^4+1$。由假设及$P\equiv1(\bmod 8)$知P不是素数。设p是P的素因数，当然p是奇数。由已证的结论知$p\equiv1(\bmod 8)$，但$p\neq p_1,\cdots,p_k$。这和假设矛盾。证毕。

例8 设p是素数，$p\equiv3(\bmod 4)$。证明：$2p+1$是素数的充要条件是

$$2^p\equiv1(\bmod 2p+1)。\tag{15}$$

证 *必要性* 若$q=2p+1$是素数，由条件知$q\equiv-1(\bmod 8)$。因而由定理3知$\left(\frac{2}{q}\right)=1$，由此及定理1(ii)得

$$1\equiv2^{(q-1)/2}\equiv2^p(\bmod 2p+1)。$$

充分性　若式(15)成立。由于p是素数，所以由第一章§3例5知，p是满足

$$2^d\equiv 1\pmod{2p+1}$$

的最小正整数d，进而由第三章§3定理3知$p\mid\phi(2p+1)$。因此必有$\phi(2p+1)=p$或$2p$。由于$2\mid\phi(m)(m>2)$，所以$\phi(2p+1)=2p$，这就证明了$2p+1$是素数（为什么）。

Legendre符号$\left(\frac{d}{p}\right)$的计算需要求出d的素因数分解式后才能利用Gauss二次互反律，这当d较大时有时是不方便的。为了克服这一缺点引进了Jacobi符号。这是下一节的内容。

习　题　六

1．计算下列Legendre符号：

$$\left(\frac{13}{47}\right),\left(\frac{30}{53}\right),\left(\frac{71}{73}\right),\left(\frac{-35}{97}\right),\left(\frac{-23}{131}\right),\left(\frac{7}{223}\right),$$

$$\left(\frac{-105}{223}\right),\left(\frac{91}{563}\right),\left(\frac{-70}{571}\right),\left(\frac{-286}{647}\right).$$

2．判断下列同余方程是否有解：

(i) $x^2\equiv 7\pmod{227}$；　　(ii) $x^2\equiv 11\pmod{511}$；

(iii) $11x^2\equiv -6\pmod{91}$；(iv) $5x^2\equiv -14\pmod{6193}$。

3．(i) 求以-3为其二次剩余的全体素数；

(ii) 求以± 3为二次剩余的全体素数；

(iii) 求以± 3为二次非剩余的全体素数；

(iv) 求以3为二次剩余、-3为二次非剩余的全体素数；

(v) 求以3为二次非剩余、-3为二次剩余的全体素数；

(vi) 求$(100)^2-3,(150)^2+3$的素因数分解式。

4．求以3为二次非剩余，2为二次剩余的全体素数（即以3为正的最小二次非剩余的全体素数）。

5．求(i) $\left(\frac{5}{p}\right)=1$的全体素数$p$；(ii) $\left(\frac{-5}{p}\right)=1$的全体素

数 p；(iii) $121^2 \pm 5, 82^2 \pm 5 \cdot 11^2, 273^2 \pm 5 \cdot 11^2$ 的素因数分解式；

(iv) $x^4 \equiv 25 (\bmod 1013)$ 是否可解。

6．求(i) $\left(\frac{-2}{p}\right) = 1$ 的全体素数 p；(ii) $\left(\frac{10}{p}\right) = 1$ 的全体素数 p。

7．(i) 求使 $x^2 \equiv 13 (\bmod p)$ 有解的全体素数 p；

(ii) 证明：$n^4 - n^2 + 1$ 的素因数 $\equiv 1 (\bmod 12)$。

8．证明下列形式的素数均有无穷多个：(i) $8k-1, 8k+3, 8k-3$；(ii) $3k+1, 6k+1, 12k+7, 12k+1$；(iii) 其十进位表示的末位数为 9．

9．设素数 $p = 4m+1, d \mid m$。证明：$\left(\frac{d}{p}\right) = 1$。

10．设素数 $p > 2$。

(i) 证明：同余方程 $(x^2-a)(x^2-b)(x^2-ab) \equiv 0 (\bmod p)$ 总有解，其中 a, b 为任意整数；

(ii) 证明：$x^6 - 11x^4 + 36x^2 - 36 \equiv 0 (\bmod p)$ 总有解。

11．设素数 $p > 2$。证明：$x^4 \equiv -4 (\bmod p)$ 有解的充要条件是

$$p \equiv 1 (\bmod 4).$$

12．证明：(i) 对任意素数 p，$x^8 \equiv 16 (\bmod p)$ 必有解；

(ii) 当 $l \geqslant 3$ 时，$x^{2^l} \equiv 2^{2^{l-1}} (\bmod p)$ 总有解。

13．(i) 设 $2 \nmid n$，奇素数 $p \mid a^n - 1$。证明：$\left(\frac{a}{p}\right) = 1$；

(ii) 设素数 $p > 2$，证明 $2^p - 1$ 的素因数 $\equiv \pm 1 (\bmod 8)$。

14．(i) 不用计算，证明：$23 \mid 2^{11} - 1, 47 \mid 2^{23} - 1, 503 \mid 2^{251} - 1$；

(ii) 若有无穷多个素数 $p = 4n+3$，使 $2p+1$ 也是素数，则有无穷多个 Mersenne 数（即形如 $2^q - 1$，q 为素数）是合数。

15．设 $q = 4^n + 1$。证明：q 是素数的充要条件是：

$$3^{(q-1)/2} \equiv -1 (\bmod q).$$

16．证明：(i) 当素数 $p = 4m+3$，$\left(\frac{a}{p}\right) = 1$ 时，$x_0 = \pm a^{m+1}$ 是

$x^2\equiv a(\bmod p)$的解；

(ii) 当 $p=8m+5$，$\left(\frac{a}{p}\right)=1$时，$x_0=\pm 2^{3m+1}a^{m+1}(2^{2m+1}+a^{2m+1})$是 $x^2\equiv a(\bmod p)$的解；

(iii) 当 $p=8m+1$，$\left(\frac{a}{p}\right)=1$时，若已知$b$使$\left(\frac{b}{p}\right)=-1$，能求出 $x^2\equiv a(\bmod p)$的解吗？

17. (i) 对 $p=11,17,19,29$，$d=2,3,5,7,13$，具体算出 § 6引理 2 中的 n 。并与 § 5例1核对结果是否相符。

(ii) 直接利用 § 6引理2证明：设素数 $p>5$，

$$\left(\frac{5}{p}\right)=(-1)^{[p/5]-[p/10]+[2p/5]-[3p/10]}.$$

18. 设素数 $p>2, p\nmid d$。再设 $p/2<j\leqslant p-1$，

$$s_j\equiv jd(\bmod p),\quad 0<s_j<p.$$

以 n'表这$(p-1)/2$个 $s_j(p/2<j\leqslant p-1)$中小于 $p/2$的 s_j的个数。证明：$\left(\frac{d}{p}\right)=(-1)^{n'}$，及 $n=n'$，n 由 § 6引理 2 给出。

19. 设素数 $p>2, p\nmid d$。再设$1\leqslant j<p/2$，

$$u_j\equiv(2j-1)d(\bmod p),\quad 0<u_j<p,$$

n_1 是这$(p-1)/2$个 u_j中为偶数的 u_j 的个数。证明：

$$\left(\frac{d}{p}\right)=(-1)^{n_1}.$$

20. 设素数 $p>2, p\nmid d$。再设$1\leqslant j<p/2$，

$$v_j\equiv 2jd(\bmod p),\quad 0<v_j<p,$$

n_1'是这$(p-1)/2$个 v_j 中为奇数的 v_j 的个数。证明：

$$\left(\frac{d}{p}\right)=(-1)^{n_1'},\quad n_1=n_1',$$

其中n_1由第19题给出。

21．对第17题给出的 p 和 d，具体算出第18—20题中的 n'，n_1, n_1'，并与 § 5例1核对结果是否相符。

22．分别直接利用第18，19，20题来求 $\left(\frac{2}{p}\right)$（即 § 6定理3），$\left(\frac{3}{p}\right)$（即 § 6例3）。

23．设 p, d 及 n' 由第18题给出，$2 \nmid d$．证明：

$$n' \equiv \sum_{p/2<j<p} \left[\frac{jd}{p}\right] \pmod 2.$$

24．设 p, d, n_1 由第19题给出，$2 \nmid d$．证明：

$$n_1 \equiv \sum_{1 \leqslant j<p/2} \left[\frac{(2j-1)d}{p}\right] \pmod 2.$$

25．设 p, d, n_1' 由第20题给出，$2 \nmid d$．证明：

$$n_1' \equiv \sum_{1 \leqslant j<p/2} \left[\frac{2jd}{p}\right] \pmod 2.$$

26．分别直接用 § 6定理4，第23，24，25题，对第17题的 p, d $(d \neq 2)$ 具体算出相应的和式及 $\left(\frac{d}{p}\right)$．并与 § 5例1核对结果是否相符。

27．设素数 $p \equiv 3 \pmod 4$．设 $1, 2, \cdots, p-1$ 中的二次剩余为偶数的数的个数记为 $R^{(2)}$．证明：

$$R^{(2)} = \begin{cases} N_1, & p \equiv 3 \pmod 8; \\ (p-1)/2 - N_1, & p \equiv 7 \pmod 8), \end{cases}$$

其中 N_1 由 § 5习题五第12题(iii)给出。

28．设素数 $p \equiv 3 \pmod 4$，R_1 是 $1, 2, \cdots, (p-1)/2$ 中模 p 的二次剩余的个数．证明：

(i) $2 \cdot 4 \cdots (p-1) \equiv (-1)^{R_1+(p-3)/4} \pmod p$；

(ii) $1\cdot 3\cdots(p-2)\equiv(-1)^{n_1+(p+1)/4}\pmod{p}$;

(iii) $((p-1)/2)!\equiv(-1)^{n_1+1}\pmod{p}$。

29．说明：为了计算 Legendre 符号，可以避免利用$\left(\frac{2}{q}\right)$的计算公式。

30．设 a,b 是整数，$b^2>1$。证明：(i) $b^2+2\nmid 4a^2+1$；

(ii) $b^2-2\nmid 4a^2+1$；　(iii) $2b^2+3\nmid a^2-2$；

(iv) $3b^2+4\nmid a^2+2$。

31．利用第19题，按下述途径来证明§6定理1。设 p,q 均为奇素数，$p\neq q$。对数对$\{j,k\}$，记 $L(j,k)=(2j-1)q-(2k-1)p$，$1\leqslant j\leqslant(p-1)/2$，$1\leqslant k\leqslant(q-1)/2$。以 n_1 表第19题中取 $p=p,d=q$ 时所定义的 n_1，以 $\bar{n}_1$ 表第19题中取 $p=q,d=p$ 时所定义的n_1。证明：

(i) 在这$(p-1)/2\cdot(q-1)/2$个不等于零的偶数 $L(j,k)$ 中有且仅有$n_1+\bar{n}_1$ 个满足条件：$-q<L(j,k)<p$；

(ii) 若 $-q<L(j,k)<p$，则

$$-q<L((p+1)/2-j,(q+1)/2-k)<p;$$

(iii) 通过把满足 (i)中条件的 $n_1+\bar{n}_1$ 对数对$\{j,k\}$，以$\{j,k\}$与$\{(p+1)/2-j,(q+1)/2-k\}$为一组来分对，证明：$n_1+\bar{n}_1$ 与$(p-1)/2\cdot(q-1)/2$的奇偶性相同。

32．设素数 $p\geqslant 3,p\nmid a$。证明：$\displaystyle\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=0$。

33．设素数 $p\geqslant 3,p\nmid a$。证明：

$$\sum_{x=1}^{p}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p}\left(\frac{x^2+x}{p}\right)=-1.$$

34．设素数 $p\geqslant 3,p\nmid a$，以及 $f(x)=ax^2+bx+c$，$\Delta=b^2-4ac$。证明：

(i) 若 $p\nmid\Delta$，则$\displaystyle\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right)=-\left(\frac{a}{p}\right)$；

(ii) 若 $p|\Delta$，则 $\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right)=(p-1)\left(\frac{a}{p}\right)$.

35. 证明：对任意素数 p，必有整数 a,b,c,d 使得：

$$x^4+1\equiv(x^2+ax+b)(x^2+cx+d)\pmod p.$$

§7 Jacobi 符号

定义1 设奇数 $P>1, P=p_1\cdots p_s, p_j(1\leqslant j\leqslant s)$ 是素数。定义

$$\left(\frac{d}{P}\right)=\left(\frac{d}{p_1}\right)\cdots\left(\frac{d}{p_s}\right),$$

这里 $\left(\frac{d}{p_j}\right)(1\leqslant j\leqslant s)$ 是模 p_j 的 Legendre 符号。我们把 $\left(\frac{d}{P}\right)$ 称为是 Jacobi 符号。

显见，当 P 本身是奇素数时，Jacobi 符号就是Legendre 符号。由定义和 Legendre 符号的基本性质立即推出（证明留给读者）：

定理1 Jacobi 符号有以下性质：

(i) $\left(\frac{1}{P}\right)=1$；当 $(d,P)>1$ 时，$\left(\frac{d}{P}\right)=0$；当 $(d,P)=1$ 时，$\left(\frac{d}{P}\right)$ 取值 ±1；

(ii) $\left(\frac{d}{P}\right)=\left(\frac{d+P}{P}\right)$；

(iii) $\left(\frac{dc}{P}\right)=\left(\frac{d}{P}\right)\left(\frac{c}{P}\right)$；

(iv) $\left(\frac{d}{P_1P_2}\right)=\left(\frac{d}{P_1}\right)\left(\frac{d}{P_2}\right)$；

(v) 当 $(P,d)=1$ 时，$\left(\frac{d^2}{P}\right)=\left(\frac{d}{P^2}\right)=1$.

为证明进一步性质需要下面的引理：

引理2 设 $a_j \equiv 1 \pmod m$ $(1 \leqslant j \leqslant s)$，$a = a_1 \cdots a_s$，我们有

$$\frac{a-1}{m} \equiv \frac{a_1-1}{m} + \cdots + \frac{a_s-1}{m} \pmod m。$$

证 显然只要证 $s=2$ 的情形。我们有

$$a - 1 = a_1 a_2 - 1 = (a_1 - 1) + (a_2 - 1) + (a_1 - 1)(a_2 - 1)。$$

由 $a_j \equiv 1 \pmod m$ 知 $a \equiv 1 \pmod m$，所以

$$\frac{a-1}{m} = \frac{a_1-1}{m} + \frac{a_2-1}{m} + \frac{(a_1-1)(a_2-1)}{m}$$

$$\equiv \frac{a_1-1}{m} + \frac{a_2-1}{m} \pmod m。$$

证毕。

定理3 我们有

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}; \tag{1}$$

$$\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}. \tag{2}$$

证 设 $P = p_1 \cdots p_s$，p_j 是奇素数。由定义及 § 6定理1(v)知

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_s}\right) = (-1)^{(p_1-1)/2 + \cdots + (p_s-1)/2}.$$

在引理 2 中取 $m = 2, a_j = p_j (1 \leqslant j \leqslant s)$，就得到

$$\frac{P-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_s-1}{2} \pmod 2. \tag{3}$$

由以上两式即得式(1)。由定义和 § 6定理3得

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_s}\right) = (-1)^{(p_1^2-1)/8 + \cdots + (p_s^2-1)/8}.$$

由于 p_j 是奇数，所以 $p_j^2 \equiv 1 \pmod 8$。在引理 2 中取 $m = 8$，

$a_j=p_j^2(1\leqslant j\leqslant s)$，就得到

$$\frac{P^2-1}{8}\equiv\frac{p_1^2-1}{8}+\cdots+\frac{p_s^2-1}{8}(\bmod 8).$$

由以上两式即得式(2)。

对 Jacobi 符号有以下的互反律成立。

定理4 设奇数 $P>1$，奇数 $Q>1,(P,Q)=1$. 我们有

$$\left(\frac{Q}{P}\right)\cdot\left(\frac{P}{Q}\right)=(-1)^{(P-1)/2\cdot(Q-1)/2}.$$

证 设 $P=p_1\cdots p_s,Q=q_1\cdots q_r,p_j,q_i$ 均为奇素数。由定义，定理1及§6定理5(注意 $q_i\neq p_j$)得

$$\left(\frac{Q}{P}\right)=\prod_{j=1}^{s}\left(\frac{Q}{p_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)(-1)^{(p_j-1)/2\cdot(q_i-1)/2}$$

$$=\left\{\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)\right\}\left\{\prod_{j=1}^{s}\prod_{i=1}^{r}(-1)^{(p_j-1)/2\cdot(q_i-1)/2}\right\},$$

$$=\left(\frac{P}{Q}\right)\prod_{j=1}^{s}(-1)^{(p_j-1)/2\cdot\sum_{i=1}^{r}(q_i-1)/2}.$$

类似于式(3)可得

$$\frac{Q-1}{2}\equiv\frac{q_1-1}{2}+\cdots+\frac{q_r-1}{2}(\bmod 2),$$

由以上两式得

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)\prod_{j=1}^{s}(-1)^{(p_j-1)/2\cdot(Q-1)/2}$$

$$=\left(\frac{P}{Q}\right)(-1)^{(Q-1)/2\cdot\sum_{j=1}^{s}(p_j-1)/2}$$

$$=\left(\frac{P}{Q}\right)(-1)^{(P-1)/2\cdot(Q-1)/2},$$

最后一步用了式(3)。注意到$(Q,P)=1$时$\left(\frac{P}{Q}\right)=\pm1$，由此就推出所要结论。

以上证明的这些性质表明：为了计算 Jacobi符号（当然包括 Legendre 符号作为它的特殊情形），我们并不需要求素因数分解式。例如，105虽然不是奇素数，当我们要计算 Legendre 符号$\left(\frac{105}{317}\right)$时，可以先把它看作是 Jacobi 符号来计算，由定理4得

$$\left(\frac{105}{317}\right)=\left(\frac{317}{105}\right)=\left(\frac{2}{105}\right)=1,$$

后两步用到了定理1(ii)及式(2)，这也就是它作为 Legendre 符号的值。因此，引进 Jacobi 符号后，对计算 Legendre 符号是十分方便的。但应该强调指出：Jacobi 符号与 Legendre符号的本质差别是：Jacobi 符号$\left(\frac{d}{P}\right)=1$，绝不表示二次同余方程

$$x^2\equiv d(\text{mod } P)$$

一定有解。例如，奇素数$p\equiv-1(\text{mod } 4)$，取$P=p^2$时总有$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p^2}\right)=1$，但

$$x^2\equiv-1(\text{mod } p)$$

无解，当然

$$x^2\equiv-1(\text{mod } p^2)$$

也无解。再比如 Jacobi 符号

$$\left(\frac{2}{3599}\right)=1,$$

但由§6例2(ii)知，同余方程

$$x^2 \equiv 2 \pmod{3599}$$

无解。由于这种差别，所以对 Jacobi 符号，§6的定理 1(ii)，引理 2 及定理 4 都不成立。

习 题 七

1．利用 Jacobi 符号性质计算：

(i) $\left(\frac{51}{71}\right)$；(ii) $\left(\frac{-35}{97}\right)$；(iii) $\left(\frac{313}{401}\right)$；(iv) $\left(\frac{165}{503}\right)$。

2．设 a,b 是正整数，$2\nmid b$。证明对 Jacobi 符号有公式：

$$\left(\frac{a}{2a+b}\right)=\begin{cases}\left(\frac{a}{b}\right), & a\equiv 0,1 \pmod 4;\\ -\left(\frac{a}{b}\right), & a\equiv 2,3 \pmod 4.\end{cases}$$

3．设 a,b,c 正整数，$(a,b)=1$，$2\nmid b$ 及 $b<4ac$。证明对 Jacobi 符号有公式：

$$\left(\frac{a}{4ac-b}\right)=\left(\frac{a}{b}\right).$$

4．整数 a 是每个素数的二次剩余的充要条件是 $a=b^2$。(做本题时假定以下结论成立：设 $m\geqslant 1,(d,m)=1$，则必有素数 $p\equiv d \pmod m$)。

§8　模为素数的高次同余方程

设 p 是素数，$n\geqslant 0$，

$$f(x)=a_nx^n+\cdots+a_0. \tag{1}$$

本节要讨论同余方程①

① 为方便起见，当 $n=0$ 时，把 $a_0\equiv 0 \pmod p$ 也看作是同余方程。当 $p\nmid a_0$，它不成立，看作无解；当 $p\mid a_0$ 时，它成立，看作解数为 p。

$$f(x)\equiv 0\pmod p \tag{2}$$

的次数和解数的关系，以及模 p 的同余方程一定可化为次数 $<p$ 的同余方程。本节所用的主要工具是整系数多项式的除法，及 Fermat 小定理(第三章 § 3式(14))，即模 p 的 p 次同余方程

$$x^p - x\equiv 0\pmod p \tag{3}$$

的解数为 p，也就是说 x 取任意整数时式(3)总成立。

定理1 设 $p\nmid a_n$。若 n 次同余方程(2)有 k 个不同的解

$$x\equiv c_1,\cdots,c_k\pmod p, \tag{4}$$

那么，一定存在唯一的一对整系数多项式 $g_k(x)$ 与 $r_k(x)$，使得

$$f(x)=(x-c_1)\cdots(x-c_k)g_k(x)+p\cdot r_k(x), \tag{5}$$

$r_k(x)$ 的次数 $<k$，$g_k(x)$ 的次数为 $n-k\geqslant 0$，且 $g_k(x)$ 的首项系数是 a_n。

证 唯一性 若还有这样的 $\bar g_k(x)$，$\bar r_k(x)$，使得

$$f(x)=(x-c_1)\cdots(x-c_k)\bar g_k(x)+p\cdot \bar r_k(x),$$

则有

$$(x-c_1)\cdots(x-c_k)(g_k(x)-\bar g_k(x))=p(\bar r_k(x)-r_k(x)).$$

若 $g_k(x)\neq\bar g_k(x)$，则左边是次数 $\geqslant k$ 的多项式，而右边的次数 $<k$，所以不可能。若 $g_k(x)=\bar g_k(x)$，则由上式推出 $r_k(x)=\bar r_k(x)$。这就证明了唯一性(事实上，以后用不到唯一性)。

存在性 对 k 用归纳法。当 $k=1$ 时，由 $p\nmid a_n$ 知必有 $n\geqslant 1$(参看上页注①)。作多项式除法可得

$$f(x)=(x-c_1)g_1(x)+s_1,$$

s_1 为一整数，$g_1(x)$ 的次数为 $n-1$，首项系数为 a_n。在上式中取 $x=c_1$，由 $f(c_1)\equiv 0\pmod p$ 即得 $p\mid s_1$，$s_1=p\cdot r_1$。这样，取 $g_1(x)$ 及 $r_1(x)=r_1$ 就满足式(5)($k=1$)。假设 $k=l(\geqslant 1)$ 时结论成立，即存在次数 $<l$ 的多项式 $r_l(x)$，及次数为 $n-l\geqslant 0$、首项系数为 a_n 的多项式 $g_l(x)$，使得

$$f(x)=(x-c_1)\cdots(x-c_l)g_l(x)+p\cdot r_l(x). \tag{6}$$

当 $k=l+1$ 时，首先由归纳假设知必有式(6)成立。在式(6)中取

$x=c_{l+1}$，由 $f(c_{l+1})\equiv 0 \pmod p$ 及 $(c_{l+1}-c_1)\cdots(c_{l+1}-c_l)\not\equiv 0 \pmod p$，从式(6)推出 $x\equiv c_{l+1} \pmod p$ 是同余方程

$$g_l(x)\equiv 0 \pmod p \qquad (7)$$

的解。由此及 $p\nmid a_n$，推出 $g_l(x)$ 的次数 $n-l\geqslant 1$。这样，对同余方程(7)利用 $k=1$ 的结论得

$$g_l(x)=(x-c_{l+1})h_1(x)+p\cdot t_1,$$

这里 $h_1(x)$ 的次数为 $(n-l)-1\geqslant 0$、首项系数为 a_n，t_1 为一整数。把上式代入式(6)即得

$$f(x)=(x-1)\cdots(x-c_{l+1})h_1(x)$$
$$+p(t_1(x-c_1)\cdots(x-c_l)+r_l(x)).$$

取 $g_{l+1}(x)=h_1(x)$，$r_{l+1}(x)=t_1(x-c_1)\cdots(x-c_l)+r_l(x)$ 就证明了结论对 $k=l+1$ 成立。证毕。

定理 1 的结论还可加强(见习题八第 1 题)。定理 1 已经证明了下面的结论：

定理2 设 $p\nmid a_n$。那么，n 次同余方程(2)的解数

$$k\leqslant \min(n,p).$$

证 解数 $\leqslant p$ 是显然的。无解(即解数为0)时结论当然成立。当解数 $k\geqslant 1$ 时，由定理 1 知存在 $g_k(x)$，$r_k(x)$ 使式(5)成立。由 $g_k(x)$ 的存在性及其次数 $n-k\geqslant 0$ 就推出 $k\leqslant n$。证毕。

定理 2 通常称为 Lagrange 定理。我们也可以不利用定理 1 而直接证明定理 2。

定理2的直接证明 对次数 n 用归纳法。显然只要证 $k\leqslant n$。当 $n=0$ 时，$f(x)=a_0$，$p\nmid a_0$，由约定(见第218页注①)知同余方程(2)无解，所以结论成立。设结论对 $n=l(\geqslant 0)$ 成立。当 $n=l+1$ 时，若结论不成立，则同余方程(2)$(n=l+1, p\nmid a_{l+1})$ 至少有 $l+2$ 个解，设为

$$x\equiv c_1, c_2, \cdots, c_{l+2} \pmod p. \qquad (8)$$

考虑多项式

$$f(x)-f(c_1)=a_{l+1}(x^{l+1}-c_1^{l+1})+\cdots+a_1(x-c_1)$$

$$= (x - c_1)(a_{l+1}x^l + \cdots) = (x - c_1)h(x). \tag{9}$$

显见，$h(x)$是 l 次多项式且$p \nmid a_{l+1}$，所以

$$h(x) \equiv 0 \pmod p \tag{10}$$

是 l 次同余方程．但由假定(8)及式(9)知，l 次同余方程(10)至少有$l+1$个解

$$x \equiv c_2, \cdots, c_{l+2} \pmod p.$$

这和归纳假设矛盾。证毕。

定理 2 的一个直接推论是

推论3 若同余方程(2)的解数$>n$，则必有$p|a_j$，$0 \leqslant j \leqslant n$。

证 用反证法。若结论不成立，则必有 d，$0 \leqslant d \leqslant n$，使得$p|a_j$，$d<j \leqslant n$，$p \nmid a_d$。这样，同余方程(2)与同余方程

$$a_d x^d + \cdots + a_0 \equiv 0 \pmod p$$

的解数相同。但由定理 2 知，它的解数$\leqslant d \leqslant n$。矛盾。证毕。

定理 1 和 2 中的条件 $p \nmid a_n$ 是十分重要的，不然定理 1 和定理 2 都不成立。例如，$f(x) = px$，$px \equiv 0 \pmod p$至少有两个解$x \equiv 0, 1 \pmod p$，所以定理 2 不成立。也不可能存在$g_2(x)$及$r_2(x)$（次数$\leqslant 1$）使得

$$px = x(x-1)g_2(x) + p \cdot r_2(x).$$

所以定理 1 也不成立。定理 1 和定理 2 中的条件 $p \nmid a_n$ 改为$p \nmid (a_n, \cdots, a_0)$，结论也成立，这时定理1中的$g_k(x)$也满足条件：$p$不能整除$g_k(x)$的系数的最大公约数（详细证明留给读者）。应该指出，从定理 2（它可以直接证明）也可推出定理 1，所以这两个定理是等价的，下面来给出这样的证明。

由定理2推出定理1的证明 由定理 2 知，必有$k \leqslant n$，所以可作多项式除法，得到

$$f(x) = (x - c_1) \cdots (x - c_k) g(x) + s(x),$$

其中$g(x)$的次数为$n-k \geqslant 0$，首项系数为a_n，以及$s(x)$的次数$<k$。由此及条件知，同余方程

$$s(x) \equiv 0 \pmod p$$

至少有由式(4)给出的k个解。因而由推论3(这是由定理2推出的)知，$s(x)$的系数均被p整除，所以$s(x)=p\cdot r(x)$。这就证明了存在性。唯一性的证明和原来的相同。证毕。

由定理1(或定理2)还可立即推出：

推论4 设$p\nmid a_n$。那么，n次同余方程(2)恰有n个解(即解数为n)：

$$x\equiv c_1,\cdots,c_n \pmod p \tag{11}$$

的充要条件是存在对模p两两不同的$c_1,c_2,\cdots,c_n$，使得

$$f(x)=a_n(x-c_1)\cdots(x-c_n)+p\cdot r(x), \tag{12}$$

其中$r(x)$是次数$<n$的整系数多项式。

证明留给读者。特别地，在推论4中取$f(x)=x^{p-1}-1$，由Fermat小定理知，$p-1$次同余方程

$$x^{p-1}-1\equiv 0 \pmod p$$

恰有$p-1$个解

$$x\equiv 1,2,\cdots,p-1 \pmod p.$$

因而由推论4得

$$x^{p-1}-1=(x-1)\cdots(x-p+1)+p\cdot r(x). \tag{13}$$

取$x=p$由式(13)即得

$$(p-1)!\equiv -1 \pmod p.$$

这就给出了Wilson定理(第三章§4定理1)的又一个证明。

下面来证明n次同余方程恰有n个解的判别法。

定理5 设$a_n=1$。那么，n次同余方程(2)的解数等于n的充要条件是

$$x^p-x=f(x)q(x)+p\cdot r(x), \tag{14}$$

其中$q(x),r(x)$是整系数多项式，且$r(x)$的次数$<n$。

证 必要性 显见$n\leqslant p$。所以作多项式除法可得：

$$x^p-x=f(x)q(x)+s(x).$$

$s(x)$的次数$<n$。由此及Fermat小定理知，同余方程(2)的解都是同余方程

$$s(x)\equiv 0 \pmod p$$

的解，因而由推论 3 推出$s(x)$的系数都是 p 的倍数，这就证明了必要性。

充分性　这时必有$n\leqslant p$(为什么)，$f(x)$是 n 次多项式，$q(x)$是$p-n$次多项式。由式(14)及Fermat小定理知，同余方程

$$f(x)q(x)\equiv 0 \pmod p$$

的解数为 p，设同余方程

$$f(x)\equiv 0 \pmod p$$

的解数为k，同余方程

$$q(x)\equiv 0 \pmod p$$

的解数为 h。因此有 $p\leqslant k+h$。但另一方面由定理 2 知，$k\leqslant n$，$h\leqslant p-n$，所以$k+h=p$。由此就推出$k=n$。证毕。

下面来举几个应用定理 5 的例子。

例 1　判断同余方程$2x^3+5x^2+6x+1\equiv 0 \pmod 7$是否有三个解。

这里首项系数为 2，先作恒等变形，可知原方程与

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3\equiv 0 \pmod 7$$

的解相同。作多项式除法可得

$$x^7-x=(x^3-x^2+3x-3)(x^3+x^2-2x-2)x+7x(x^2-1).$$

所以，原同余方程的解数为 3。

例 2　设素数$p>2$，$p\nmid d$。求二次同余方程

$$x^2-d\equiv 0 \pmod p \tag{15}$$

的解数为 2 的充要条件。

解　由于

$$\begin{aligned}x^{p-1}-1&=(x^2)^{(p-1)/2}-d^{(p-1)/2}+d^{(p-1)/2}-1\\&=(x^2-d)q(x)+d^{(p-1)/2}-1,\end{aligned}$$

所以由定理 5 知，解数为 2 的充要条件是

$$d^{(p-1)/2}-1\equiv 0 \pmod p. \tag{16}$$

由于$p>2$，所以同余方程(15)要末无解，要末有解且解数必为 2。所以，(16)也是(15)有解的充要条件。这就给出了 Euler 判

别法(§5定理2)的又一证明。此外，注意到

$$x^{p-1}-1=(x^{(p-1)/2}-1)(x^{(p-1)/2}+1),$$

所以同余方程(16)(把 d 看作 x)的解数为$(p-1)/2$，即模$p(>2)$的二次剩余恰有$(p-1)/2$个。这就给出了§5定理1的又一证明。这种证明方法，对二次剩余来说似乎"太高级"，但在讨论高次剩余(见定理7,8,9)时，这种一般方法就显出了优越性。

虽然可以出现任意次的模 p 的同余方程，但下面的定理表明我们总可以把它化为次数$<p$的同余方程。

定理6 (i) 同余方程(2)的解数为 p 的充要条件是

$$f(x)=(x^p-x)g(x)+p\cdot r(x), \tag{17}$$

其中整系数多项式$r(x)$的次数$<p$；

(ii) 同余方程(2)的解数$<p$的充要条件是存在一个次数$<p$、首项系数为1的整系数多项式$f^*(x)$，使得同余方程(2)与同余方程

$$f^*(x)\equiv 0 \pmod p \tag{18}$$

的解相同。同余方程(18)称为是同余方程(2)的**等价同余方程**。

证 先证(i)。充分性由式(17)及 Fermat 小定理推出。由多项式除法可得

$$f(x)=(x^p-x)g(x)+s(x), \tag{19}$$

其中$s(x)$是次数$<p$的整系数多项式。由同余方程(2)的解数为 p 及Fermat小定理推出：同余方程

$$s(x)\equiv 0 \pmod p \tag{20}$$

的解数也为 p。由此及推论3推出 $s(x)=p\cdot r(x)$，$r(x)$为次数$<p$的整系数多项式。这就证明了必要性。

再来证(ii)。充分性由定理2推出。下证必要性。这时同样有式(19)成立。由此及 Fermat 小定理知，同余方程(2)与(20)的解相同。因此，同余方程(20)的解数$<p$，进而推出$s(x)$的系数一定不能全被 p 整除(为什么)。设

$$s(x)=b_lx^l+\cdots+b_0, \qquad 0\leqslant l<p,$$

一定有$0\leqslant d\leqslant l$使得$p\mid b_j$，$d<j\leqslant l$，$p\nmid b_d$。这样，同余方程(20)就与同余方程

$$b_dx^d+\cdots+b_0\equiv0\pmod p,\qquad 0\leqslant d<p \qquad (21)$$

的解相同。取b_d^{-1}是b_d对模p的逆，$b_d^{-1}b_d=1+e\cdot p$，这样，由

$$\begin{aligned}f^*(x)&=b_d^{-1}(b_dx^d+\cdots+b_0)-e\cdot px^d\\&=x^d+b_d^{-1}b_{d-1}x^{d-1}+\cdots+b_d^{-1}b_0,\end{aligned}$$

所得的同余方程(18)就和同余方程(2)的解相同。这就证明了必要性。证毕。

这样，对于一个同余方程(2)可以按以下步骤来简化：先去掉其中系数为p的倍数的项；如果所得到的等价的同余方程的次数$\geqslant p$，那末，再按定理5作多项式除法(19)，就可确定它的解数是否为p。若不是p，就可进一步找出次数$<p$的等价同余方程(18)。下面来举几个例子。

例3 简化同余方程

$$21x^{18}+2x^{15}-x^{10}+4x-3\equiv0\pmod 7.$$

解 先去掉系数为7的倍数的项得

$$2x^{15}-x^{10}+4x-3\equiv0\pmod 7.$$

作多项式除法(19)($p=7$)得：

$$\begin{aligned}2x^{15}-x^{10}+4x-3=&(x^7-x)(2x^8-x^3+2x^2)\\&+(-x^4+2x^3+4x-3).\end{aligned}$$

由此就得到等价同余方程

$$x^4-2x^3-4x+3\equiv0\pmod 7.$$

由直接代入$x=0,\pm1,\pm2,\pm3$计算知，同余方程无解。

为了求出等价同余方程，我们并不需要知道多项式除法(19)中的$g(x)$，而且当次数较高时，做这种除法是很麻烦的。事实上，我们可以利用恒等同余式(3)(即Fermat小定理)来直接化简，以求得等价同余方程。

例4 简化同余方程

$$f(x)=3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3$$

$$+12x^2+x\equiv 0 \pmod 5).$$

解　由恒等同余式(3)($p=5$)可得

$$x^{14}\equiv x^6\equiv x^2 \pmod 5, \qquad x^{13}\equiv x^5\equiv x \pmod 5,$$

$$x^{11}\equiv x^3 \pmod 5, \qquad x^9\equiv x^5\equiv x \pmod 5,$$

$$x^6\equiv x^2 \pmod 5.$$

因而原同余方程等价于

$$3x^3+16x^2+6x\equiv 0 \pmod 5.$$

进而等价于

$$2(3x^3+16x^2+6x)\equiv x^3+2x^2+2x\equiv 0 \pmod 5.$$

由直接计算知，解为$x\equiv 0,1,2 \pmod 5$。如果利用多项式除法可得：

$$f(x)=(x^5-x)(3x^9+4x^8+2x^6+3x^5+5x^4$$
$$+2x^2+4x+5)+(3x^3+16x^2+6x).$$

得到同样的结果。

作为本节结果的一个应用，我们来讨论**模为素数 p 的二项同余方程**：

$$x^n-a\equiv 0 \pmod p, \qquad p\nmid a,$$

即

$$x^n\equiv a \pmod p, \qquad p\nmid a. \tag{22}$$

当同余方程(22)有解时，a 称为是**模p的n次剩余**；无解时，称为是**模p的n次非剩余**。在§5中已经讨论了模 p 的二次剩余，先来举一个例子。取$p=11$，$n=2,4,5$。表1列出了x^2,x^4,x^5对模11的剩余。

表　1　　　　(mod 11)

x	−5	−4	−3	−2	−1	1	2	3	4	5
x^2	3	5	−2	4	1	1	4	−2	5	3
x^4	−2	3	4	5	1	1	5	4	3	−2
x^5	−1	−1	−1	1	−1	1	−1	1	1	1

由表 1 可以看出：模11的 2 次和 4 次剩余均为1，-2，3，4，5，而 2 次和 4 次非剩余均为 -1，2，-3，-4，-5；对每个 2 次或4次剩余 a，同余方程(22)恰有两个解。模11的 5 次剩余仅有 -1，1，而 ±2，±3，±4，±5 均为 5 次非剩余，对每个 5 次剩余，同余方程(22)恰有五个解。

定理7 若$n|p-1$，则同余方程(22)有解的充要条件是

$$a^{(p-1)/n}\equiv 1(\bmod p), \tag{23}$$

并且在有解时解数为 n。

证 *必要性* 若x_0是(22)的解，由$p\nmid a$知$p\nmid x_0$，由此及Fermat小定理就推出

$$a^{(p-1)/n}\equiv(x_0^n)^{(p-1)/n}\equiv x_0^{p-1}\equiv 1(\bmod p).$$

充分性 若式(23)成立，则有

$$\begin{aligned} x^{p-1}-1&=(x^n)^{(p-1)/n}-a^{(p-1)/n}+a^{(p-1)/n}-1 \\ &=(x^n)^{(p-1)/n}-a^{(p-1)/n}+p\cdot c, \end{aligned} \tag{24}$$

c 为一整数。由此知必有整系数多项式$q(x)$使得

$$x^p-x=(x^n-a)q(x)+p\cdot cx.$$

由此及定理 5 就推出(22)有解且解数为 n（事实上，由式(24)的第一式及定理 5 也推出必要性）。

上面对模11所举的例中，$n=2,5$就是定理 7 的情形，实际计算和结论相符。

定理8 若$n\nmid p-1$，则同余方程(22)有解的充要条件是同余方程

$$x^k\equiv a(\bmod p),\qquad p\nmid a \tag{25}$$

有解，其中$k=(n,p-1)$，且两者的解数相同。也就是说同余方程(22)有解的充要条件是

$$a^{(p-1)/k}\equiv 1(\bmod p), \tag{26}$$

且有解时解数为k。

证 由第一章§4定理13知，存在正整数r,s使得

$$k = r \cdot n - s \cdot (p-1)。 \tag{27}$$

若(22)有解$x=c$，则$x=c^{n/k}$是(25)的解；反之，若(25)有解 $x=e$，则由式(27)知，

$$(e^r)^n = e^k \cdot e^{s(p-1)} \equiv a \pmod p,$$

最后一步用到了$p \nmid e$及Fermat小定理，这推出$x=e^r$是(22)的解。这就证明了(22)有解的充要条件是(25)有解，由此及定理 7 推出：(22)有解的充要条件是式(26)成立。现设(22)有解，这时式(26)成立。若$x=c$是(22)的解，由式(27)知

$$c^k \equiv c^{k+s(p-1)} \equiv c^{nr} \equiv a^r \pmod p,$$

这里用到了$p \nmid c$及Fermat小定理，所以$x=c$一定是同余方程

$$x^k \equiv a^r \pmod p \tag{28}$$

的解。由定理 7 知(28)的解数为k，所以(22)的解数$\leqslant k$。反之，若$x=d$是(28)的解，则由式(27)，$p \nmid d$及Fermat小定理知

$$a^r \equiv d^k \equiv d^{k+s(p-1)} \pmod p。$$

进而有

$$a^{r \cdot n/k} \equiv d^{(k+s(p-1)) \cdot n/k} \pmod p。$$

由此及式(27)得

$$a^{1+s(p-1)/k} \equiv d^{n+(sn/k)(p-1)} \pmod p。$$

由式(26)，$p \nmid d$及Fermat小定理，从上式得到

$$a \equiv d^n \pmod p,$$

即$x=d$一定是(22)的解。这就证明了：**在(22)有解的条件下，同余方程(22)与(28)的解与解数相同**。由定理 7 知(28)的解数为k，所以(22)的解数也是k。证毕。

上面对模11所举的例中，$n=4$就是定理 8 的情形，实际计算和结论相符。

由定理 7 、定理 8 (式(26))就可以立即推出(证明留给读者)：

定理9 在模p的一个既约剩余系中，模p的n次剩余的元素个数是$(p-1)/(n, p-1)$。

现设$n|p-1$。当$n>2$时，对模p的n次非剩余a，不一定像$n=2$的情形那样，总有

$$a^{(p-1)/n}\equiv -1 \pmod p$$

成立。例如，对$p=11$，$n=5$。这时$(p-1)/n=2$，对模11的5次非剩余有

$$(\pm 2)^2\equiv 4 \pmod{11},\quad (\pm 3)^2\equiv -2 \pmod{11},$$
$$(\pm 4)^2\equiv 5 \pmod{11},\quad (\pm 5)^2\equiv 3 \pmod{11}$$

(为什么这里一个同余于-1的也没有)。容易证明“两个n次剩余相乘仍是n次剩余；一个n次剩余与一个n次非剩余相乘一定是n次非剩余(证明留给读者)。但两个n次非剩余相乘，当$n>2$时，就不一定是n次剩余了。例如：对模11来说，$(\pm 2)\cdot(\pm 3)$就都不是5次剩余，而$(\pm 2)\cdot(\pm 5)$就都是5次剩余。这里呈现出很复杂的情形。

对于判断a是否是模p的二次剩余，我们可以通过计算Legendre符号(或Jacobi符号)来确定，这时有一个很方便的算法。Gauss想对$n(>2)$次剩余来寻找类似的算法，他考虑了$n=3,4$的情形。他发现这是一个极为困难的问题，同二次剩余完全不一样，在现有的整数：$0,\pm 1,\pm 2,\cdots$范围内无法讨论这个问题，必须研究新的“整数”，这就导致对代数数与代数数论的研究(参看潘承洞和潘承彪：初等代数数论，山东大学出版社，1992)。

最后，要指出的是：在下一章讨论了原根后，定理7与定理8很容易利用原根的理论来证明。

习 题 八

1. 在§8定理1的条件下，一定存在唯一的一组正整数$\alpha_1,\cdots,\alpha_k$，及一对整系数多项式$h_k(x)$与$s_k(x)$，使得

$$f(x)=(x-c_1)^{\alpha_1}\cdots(x-c_k)^{\alpha_k}h_k(x)+p\cdot s_k(x),$$

这里$s_k(x)$的次数$<\alpha_1+\cdots+\alpha_k\leqslant n$；$h_k(x)$的次数等于

$n-(\alpha_1+\cdots+\alpha_k)\geqslant 0$，首项系数是 a_n，且满足

$$h_k(c_j)\not\equiv 0(\bmod p),\quad j=1,\cdots,k。$$

2. 求下列同余方程 $f(x)\equiv 0(\bmod p)$ 的全部解，并把 $f(x)$ 表成§8定理1，及上题中的形式：

(i) $f(x)=14x^5-6x^4+8x^3+6x^2-13x+5$，$p=7$；

(ii) $f(x)=3x^4+3x^3+x+9$，$p=7$；

(iii) $f(x)=x^7+10x^6+x^5+20x^4+8x^3-18x^2+3x+1$，

$p=13$。

3. 设素数 $p\nmid a_n$，同余方程 $a_nx^n+\cdots+a_0\equiv 0(\bmod p)$ 恰有 n 个解：$x\equiv c_1,\cdots,c_n(\bmod p)$。再设

$$\sigma_1=\sum_{i=1}^{n}c_i;\quad \sigma_2=\sum_{1\leqslant i<j\leqslant n}c_ic_j,\cdots,\sigma_n=c_1\cdots c_n。$$

证明：$a_{n-j}\equiv(-1)^ja_n\sigma_j(\bmod p)$，$1\leqslant j\leqslant n$。

4. 利用§8定理5证明：

(i) $2x^3-x^2+3x+11\equiv 0(\bmod 5)$ 的解数为3；

(ii) $x^6-4x^5+6x^4+6x^3+3x^2-2x+3\equiv 0(\bmod 13)$ 的解数为6。

5. 求下列同余方程的等价同余方程：

(i) $3x^{11}+3x^8+5\equiv 0(\bmod 7)$；

(ii) $4x^{20}+3x^{15}+2x^7+3x-2\equiv 0(\bmod 5)$；

(iii) $2x^{15}-3x^{10}+8x^6+7x^5+6x^3+2x-8\equiv 0(\bmod 7)$；

(iv) $2x^{17}+5x^{16}+3x^{14}+5x^{12}+6x^{10}+2x^9+5x^8+9x^7+22x^6$
$+3x^4+6x^3-5x^2+12x+3\equiv 0(\bmod 11)$。

6. 列出下列素数 p 的 n 次剩余：

(i) $p=7,n=2,3,4,5$；

(ii) $p=13,n=2,3,4,5$；

(iii) $p=17,n=2,3,4,8$；

(iv) $p=19,n=2,3,4,5,6$。并验证定理7、8、9的结论。

7．利用上题举出两个 n 次非剩余的乘积不一定是 n 次剩余的例子．

8．设 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，$(m,a)=1$．

(i) 证明：当 $(m,n)=1$ 时，同余方程 $x^n\equiv1 \pmod m$ 的解数为 $(n,p_1-1)\cdot(n,p_2-1)\cdots(n,p_r-1)$；

(ii) 当 $x=c_0$ 是 $x^n\equiv a \pmod m$ 的一个解时，它的全部解为 $x\equiv c_0y \pmod m$，y 是 $y^n\equiv1 \pmod m$ 的解．

9．举例说明§8中的同余方程(28)有解，不一定同余方程(22)有解．

第五章　指数与原根

本章是应用同余方程理论来研究既约剩余系的构造。在§1中引进并讨论指数的概念与性质，指数是刻画模m的既约剩余系中的元素的特征的一个量；指数等于$\phi(m)$的元素称为是模m的原根。在§2中讨论模m存在原根的充要条件及求原根的算法；当模m存在原根g时，$g^0,g,g^2,\cdots,g^{\phi(m)-1}$就给出了模$m$的一组既约剩余系，因而给出了既约剩余系的一个十分简单且便于研究的形式。在§3中，通过引进指标、指标组的概念及其性质的讨论，对一般模m的既约剩余系也给出了一个类似的简单的构造形式；§4是介绍如何利用指标和指标组来解二项同余方程。

§1　指　　数

我们已经多次讨论了以下的问题：设$m\geqslant1,(a,m)=1$。那么，必有正整数d使得

$$a^d\equiv1(\bmod m). \tag{1}$$

若d_0是使式(1)成立的最小正整数d，则对任意的使(1)成立的正整数d，必有

$$d_0\mid d \text{ 即 } d\equiv0(\bmod d_0). \tag{2}$$

在第一章§3例5(ii)中讨论了$a=2$的情形。在第一章§4例7中完全证明了这一结论，并指出当$m\geqslant2$时，$d_0\leqslant m-1$。在第三章§3定理3(Fermat-Euler定理)中证明了：对任意的$(a,m)=1$，当$d=\phi(m)$时式(1)必成立。对给定的模m，d_0是由a唯一确定的，是a的函数，d_0是刻画（与m既约的）a关于模m的性质的一个十分重要的

量(在第三章§3定理4对此作了极初步的讨论),为此.我们引进以下概念:

定义1 设 $m\geqslant 1$,$(a,m)=1$.使式(1)成立的最小正整数 d 称为 **a 对模 m 的指数**(或阶),把它记作 $\delta_m(a)$.

定义2 当 $\delta_m(a)=\phi(m)$ 时,称 a 是**模 m 的原根**.

首先来举几个例子.$m=1$ 时,所有整数的指数均为1,且均为原根.我们不讨论这种显然情形.

例1 $m=7$,$\phi(7)=6$.

a	-3	-2	-1	1	2	3
$\delta_7(a)$	3	6	2	1	3	6

由表知,原根为 $-2,3 \pmod 7$.这样的表称为是模 $m(=7)$ 的指数表.

例2 $m=10=2\cdot 5$,$\phi(10)=4$.模10的指数表是:

a	-3	-1	1	3
$\delta_{10}(a)$	4	2	1	4

由表知原根为 $\pm 3 \pmod{10}$.

例3 $m=15=3\cdot 5$,$\phi(15)=8$.模15的指数表是:

a	-7	-4	-2	-1	1	2	4	7
$\delta_{15}(a)$	4	2	4	2	1	4	2	4

由表知无原根.

例4 $m=9=3^2$,$\phi(9)=6$.模9的指数表是:

a	-4	-2	-1	1	2	4
$\delta_9(a)$	6	3	2	1	6	3

由表知原根为 $-4,2 \pmod{3^2}$。

例 5 $m=8=2^3, \phi(8)=4$。模 8 的指数表是：

a	-3	-1	1	3
$\delta_8(a)$	2	2	1	2

由表知无原根。

例 6 由第三章 § 3例 1 中的式(20)知，当 $l \geqslant 3$时，模 2^l 无原根，$\delta_{2^l}(5)=2^{l-2}$。由直接验算知，$m=2$ 时原根为 1，$m=2^2=4$时，-1是原根。

下面来列出指数的基本性质，有的前面已经证明，有的则是显然的，以后经常要应用。

性质1 若 $b \equiv a \pmod{m}$，$(a,m)=1$，则

$$\delta_m(b)=\delta_m(a).$$

性质2 若式(1)成立，则有

$$\delta_m(a) \mid d \quad 即 \quad d \equiv 0 \pmod{\delta_m(a)}.$$

性质3 $\delta_m(a) \mid \phi(m)$，$\delta_{2^l}(a) \mid 2^{l-2}$，$l \geqslant 3$。

性质4 若 $(a,m)=1$，

$$a^k \equiv a^h \pmod{m},$$

则

$$k \equiv h \pmod{\delta_m(a)}.$$

性质5 若 $(a,m)=1$，则

$$a^0, a^1, \cdots, a^{\delta_m(a)-1}$$

这 $\delta_m(a)$ 个数对模 m 两两不同余。特别地，当 a 是模 m 的原根时，即 $\delta_m(a)=\phi(m)$ 时，这 $\phi(m)$ 个数是模 m 的一组既约剩余系。

性质 5 是第三章 § 3定理 4 的一部分。其它的证明留给读者。下面来证明进一步的性质。

性质6 设 a^{-1} 是 a 对模 m 的逆，即

$$a^{-1}a \equiv 1 \pmod{m}.$$

我们有

$$\delta_m(a^{-1})=\delta_m(a).$$

证 这由
$$a^d\equiv 1(\bmod m)$$
成立的充要条件是
$$(a^{-1})^d\equiv 1(\bmod m)$$
立即推出。

性质7 设 k 是非负整数，则有
$$\delta_m(a^k)=\frac{\delta_m(a)}{(\delta_m(a),k)}. \tag{3}$$
此外，在模 m 的一个既约剩余系中，至少有 $\phi(\delta_m(a))$ 个数对模 m 的指数等于 $\delta_m(a)$。

证 记 $\delta=\delta_m(a),\delta'=\delta/(\delta,k),\delta^*=\delta_m(a^k)$。由定义知
$$a^{k\delta^*}\equiv 1(\bmod m),\quad a^{k\delta'}\equiv 1(\bmod m).$$
因而由性质 2 得
$$\delta\mid k\delta^*,\quad \delta^*\mid\delta'.$$
由第一式得
$$\delta'=\frac{\delta}{(\delta,k)}\Big|\frac{k}{(\delta,k)}\delta^*,$$
因而 $\delta'\mid\delta^*$，所以，$\delta^*=\delta'$，即式(3)成立。当 $(k,\delta_m(a))=1$ 时，$\delta_m(a^k)=\delta_m(a)$，由此及性质 5 就证明了后一部分结论。

性质8 $\delta_m(ab)=\delta_m(a)\delta_m(b)$ 的充要条件是 $(\delta_m(a),\delta_m(b))=1$。

证 设 $\delta'=\delta_m(a),\delta''=\delta_m(b),\delta=\delta_m(ab),\eta=[\delta_m(a),\delta_m(b)]$。

充分性 我们有
$$1\equiv(ab)^{\delta}\equiv(ab)^{\delta\delta''}\equiv a^{\delta\delta''}(\bmod m),$$
所以，$\delta'\mid\delta\delta''$，由此及 $(\delta',\delta'')=1$ 推出 $\delta'\mid\delta$。同样，有
$$1\equiv(ab)^{\delta}\equiv(ab)^{\delta\delta'}\equiv b^{\delta\delta'}(\bmod m),$$
所以，$\delta''\mid\delta\delta'$，由此及 $(\delta',\delta'')=1$，推出 $\delta''\mid\delta$。进而，由 $\delta'\mid\delta,\delta''\mid\delta$ 及 $(\delta',\delta'')=1$ 推出 $\delta'\delta''\mid\delta$。此外，显然有

$$(ab)^{\delta'\delta''}\equiv 1 \pmod m,$$

所以，$\delta\mid\delta'\delta''$。因此 $\delta=\delta'\delta''$。

必要性　我们有

$$(ab)^{\eta}\equiv 1 \pmod m,$$

所以 $\delta\mid\eta$。另一方面显然有 $\eta\mid\delta'\delta''$。由此及 $\delta=\delta'\delta''$ 就推出 $\eta=\delta'\delta''$，即 $(\delta',\delta'')=1$。证毕。

性质9　(i) 若 $n\mid m$，则 $\delta_n(a)\mid\delta_m(a)$；

(ii) 若 $(m_1,m_2)=1$，则有

$$\delta_{m_1m_2}(a)=[\delta_{m_1}(a),\delta_{m_2}(a)]. \tag{4}$$

证　(i) 可由性质 2 直接推出。由(i)即得 $\delta^*\mid\delta_{m_1m_2}(a)$，这里 $\delta^*=[\delta_{m_1}(a),\delta_{m_2}(a)]$。另一方面，显然有 $a^{\delta^*}\equiv 1 \pmod{m_j}$，$j=1,2$。由此及 $(m_1,m_2)=1$ 推出 $a^{\delta^*}\equiv 1 \pmod{m_1m_2}$。因而由性质 2 推出 $\delta_{m_1m_2}(a)\mid\delta^*$。所以式(4)成立。证毕。

显见，式(4)可推广为：若 $m_1,\cdots,m_s$ 两两既约，$m=m_1\cdots m_s$，则

$$\delta_m(a)=[\delta_{m_1}(a),\cdots,\delta_{m_s}(a)]. \tag{5}$$

由此，及性质 3 立即推出：

$$\delta_m(a)\mid[\phi(m_1),\cdots,\phi(m_s)]. \tag{6}$$

特别地，当 $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，$p_j$ 是不同的奇素数，我们有

$$\delta_m(a)\mid[2^{c_0},\ \phi(p_1^{\alpha_1}),\cdots,\ \phi(p_r^{\alpha_r})]=\lambda(m), \tag{7}$$

其中

$$c_0=\begin{cases}0, & \alpha_0=0,1;\\ 1, & \alpha_0=2;\\ \alpha_0-2, & \alpha_0\geqslant 3.\end{cases} \tag{8}$$

此外，利用式(4)可计算指数。例如，由例 1 和例 3 可得

$$\delta_{105}(-2)=[\delta_7(-2),\delta_{15}(-2)]=[6,4]=12.$$

性质10 设 $(m_1,m_2)=1$。那么，对任意的 a_1,a_2，必有 a 使得

$$\delta_{m_1m_2}(a)=[\delta_{m_1}(a_1),\delta_{m_2}(a_2)].$$

证 考虑同余方程组

$$x\equiv a_1(\bmod m_1),\quad x\equiv a_2(\bmod m_2).$$

由孙子定理（第四章§3定理1）知，这同余方程组有唯一解：

$$x\equiv a(\bmod m_1m_2).$$

显然有 $\delta_{m_1}(a)=\delta_{m_1}(a_1),\delta_{m_2}(a)=\delta_{m_2}(a_2)$。由此从性质9就推出所要结论。

对于模 m 来说，不一定有

$$\delta_m(ab)=[\delta_m(a),\delta_m(b)]$$

成立。例如，由例2知

$$\delta_{10}(3\cdot3)=2\neq[\delta_{10}(3),\delta_{10}(3)]=4.$$

$$\delta_{10}(3\cdot7)=1\neq[\delta_{10}(3),\delta_{10}(7)]=4.$$

但有

$$\delta_{10}(3\cdot9)=4=[\delta_{10}(3),\delta_{10}(9)]=4.$$

$$\delta_{10}(7\cdot9)=4=[\delta_{10}(7),\delta_{10}(9)]=4.$$

一般可证明以下结论。

性质11 对任意的 a,b，一定存在 c，使得

$$\delta_m(c)=[\delta_m(a),\delta_m(b)].$$

证 设 $\delta'=\delta_m(a),\delta''=\delta_m(b),\eta=[\delta',\delta'']$。一定可以把 δ'，δ'' 作这样的分解（为什么）：

$$\delta'=\tau'\eta',\quad \delta''=\tau''\eta'',$$

使得

$$(\eta',\eta'')=1,\quad \eta'\eta''=\eta.$$

由性质7知

$$\delta_m(a^{\tau'})=\eta',\quad \delta_m(b^{\tau''})=\eta''.$$

这样，由性质8推出

$$\delta_m(a^{\tau'}b^{\tau''})=\delta_m(a^{\tau'})\delta_m(b^{\tau''})=\eta'\eta''=\eta.$$

因此，取 $c=a^{\tau'}b^{\tau''}$ 就满足要求。

由式(7)可推原根存在的必要条件。

性质12 模 m 存在原根的必要条件是：

$$m=1,2,4,p^{\alpha},2p^{\alpha}, \tag{9}$$

其中 p 是奇素数。

证 当 m 不属于式(9)列出的情形时，必有

$$m=2^{\alpha}(\alpha\geqslant 3),\quad 2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}(\alpha\geqslant 2,r\geqslant 1),$$

或

$$2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}(\alpha\geqslant 0,r\geqslant 2), \tag{10}$$

其中 p_j 为不同的奇素数，$\alpha_j\geqslant 1(1\leqslant j\leqslant r)$。设 $\lambda(m)$ 由式(7)给出，容易验证，当 m 属于式(10)列出的任一情形时，必有

$$\lambda(m)<\phi(m), \tag{11}$$

由此及式(7)知，这时模 m 没有原根。

下节将证明：当 m 由式(9)给出时，模 m 必有原根存在。

习 题 一

1. 设 $m=5,11,12,13,14,15,17,19,20,21,23,36,40,63$。

(i) 列出模 m 的指数表；

(ii) 如果模 m 有原根，找出模 m 的最小正剩余系中的所有原根，及模 m 的最小正原根；

(iii) 如果模 m 没有原根，找出模 m 的最小正剩余系中所有对模 m 的指数为最大的整数。把这个最大的指数和 $\lambda(m)$（见§1式(7)）的值相比较。

2. 求 $\delta_{41}(10),\delta_{43}(7),\delta_{55}(2),\delta_{65}(8),\delta_{91}(11),\delta_{69}(4),\delta_{231}(5)$。

3. 设 $\lambda(m)$ 由§1式(7)给出。

(i) 求出所有正整数 m，使得 $\lambda(m)=1,2,3,4,5,6,7,8,12$；

(ii) 当 $(m,n)=1$ 时，$\lambda(mn)=[\lambda(m),\lambda(n)]$；

(iii) 设 d 是给定的正整数，m 是使 $\lambda(n)=d$ 的最大正整数 n，

证明：当 $\lambda(n)=d$ 时，必有 $n\mid m$。

4．证明：3 是1459的最小正原根。

5．设 $m=37,43$．求出模 m 的最小正剩余系中所有指数为 6 的整数。

6．设 $m\geqslant1,n\geqslant1$，及 $(n,\phi(m))=1$。证明：当 x 遍历模 m 的既约剩余系时，x^n 也遍历模 m 的既约剩余系。

7．设素数$p>2$，证明：$\delta_p(a)=2$的充要条件是$a\equiv-1(\bmod p)$。这结论对合数模成立吗？

8．设 p 为素数，$\delta_p(a)=3$。证明：$\delta_p(1+a)=6$。

9．若 $\delta_m(a)=m-1$，则 m 是素数。

10．设 p 为素数，$\delta_p(a)=h$。证明：

(i) 若 $2\mid h$，则 $a^{h/2}\equiv-1(\bmod p)$；

(ii) 若 $4\mid h$，则 $\delta_p(-a)=h$；

(iii) 若 $2\mid h,4\nmid h$，则 $\delta_p(-a)=h/2$。

11．设素数 $p\equiv1(\bmod 4)$。若 g 为模 p 的原根，则 $-g$ 也是原根。

12．若素数 $p\equiv3(\bmod 4)$，则 g 为模 p 的原根的充要条件是

$$\delta_p(-g)=(p-1)/2.$$

13．设 $m=2^\alpha,\alpha\geqslant3$，再设 $1\leqslant j\leqslant\alpha-2$。求整数 a 使 $\delta_m(a)=2^j$。

14．设 $m=2^\alpha,\alpha\geqslant4$。证明：$\delta_m(a)=2^{\alpha-2}$ 的充要条件是 $a\equiv\pm3(\bmod 8)$。

15．设第 n 个 Fermat 数 $F_n=2^{2^n}+1$。证明：

(i) $\delta_{F_n}(2)=2^{n+1}$；

(ii) 若素数 $p\mid F_n$，则 $\delta_p(2)=2^{n+1}$；

(iii) F_n 的素因数 $p\equiv1(\bmod 2^{n+1})$；

(iv) 若F_n 是素数，$n>1$，则 2 一定不是 F_n 的原根；

(v) 若 F_n 是素数，则模 F_n 的任一二次非剩余必为 F_n 的原根；

(vi) 若 F_n 是素数，则 $\pm 3, \pm 7$ 都是原根。

16. 设 p, q 是素数，证明：

(i) 若 $q \equiv 1 \pmod 4$，$p = 2q + 1$，则 2 是模 p 的原根；

(ii) 若 $q \equiv -1 \pmod 4$，$p = 2q + 1$，则 -2 是模 p 的原根；

(iii) 若 $q \equiv 1 \pmod 2$，$q > 3$，$p = 2q + 1$，则 -3，-4 都是模 p 的原根；

(iv) 若 $q \equiv 1 \pmod 2$，$p = 4q + 1$，则 2 是模 p 的原根；

(v) 分别对每种情形举出两个实例来验证结论。

17. 设素数 $p = 2^m + 1$。证明：模 p 的二次非剩余 a 一定是模 p 的原根。

18. 若 $3 < q \equiv 3 \pmod 4$，$p = 2q + 1$ 都是素数，则至少有三个相邻整数都是模 p 的原根。举出两个实例具体说明结论。

19. 设 $m > 1$，$(ab, m) = 1$。再设 λ 是使 $a^d \equiv b^d \pmod m$ 成立的最小正整数 d。证明：(i) $\lambda \mid \phi(m)$；(ii) 若 $a^k \equiv b^k \pmod m$，则 $\lambda \mid k$。

20. 设 $n > 1$，$a > b \geqslant 1$。证明：

(i) $a^n - b^n$ 的素因数一定要么是形如 $kn + 1$，要么是 $a^{n_1} - b^{n_1}$ 的因数，$n_1 \mid n$，$n_1 < n$；

(ii) $a^n + b^n$ 的素因数一定要么是形如 $2kn + 1$，要么是 $a^{n_1} + b^{n_1}$ 的因数，这里 $n_1 < n$，$n_1 \mid n$，$(n/n_1, 2) = 1$；

(iii) $F_n = 2^{2^n} + 1$ 的素因数必为 $2^{n+1}k + 1$ 的形式。

21. 设 $m > 1$，$c \geqslant 1$，$(a, m) = 1$。再设 $\delta_m(a^c) = d$，试决定 $\delta_m(a)$ 的值所应满足的条件，及这种可能取到的值的个数。

22. 设 $m > 1$，$(ab, m) = 1$，及 $\lambda = (\delta_m(a), \delta_m(b))$。证明：

(i) $\lambda^2 \delta_m((ab)^{\lambda}) = \delta_m(a)\delta_m(b)$；

(ii) $\lambda^2 \delta_m(ab) = (\delta_m(ab), \lambda)\delta_m(a)\delta_m(b)$。

23. 设 q, p 均为奇素数，$p = 4q + 1$。证明：

(i) 同余方程 $x^2 \equiv -1 \pmod p$ 恰有两解，且都是模 p 的二次非剩余；

(ii) 模 p 的所有二次非剩余中，除了(i)中同余方程的两个解之外，都是模 p 的原根；

(iii) 用以上方法求 29,53 的所有原根。

24. 设 $n\geqslant 1$, q, p 均为奇素数，$p=2^n q+1$。再设 a 是模 p 的二次非剩余，且满足 $a^{2^n}\not\equiv 1 \pmod p$。证明：$a$ 是 p 的原根。

25. 设素数 $p>2$, $\delta_p(a)=4$。求 $(a+1)^4$ 对模 p 的最小正剩余。

26. 证明：(i) $2^{17}-1=131071$ 是素数；

(ii) $(2^{19}+1)/3$ 是素数。

27. 设素数 $p>2$, g 是 p 的原根。证明：存在正整数 k，使得 $g^{k+1}\equiv g^k+1 \pmod p$。

28. 设素数 $p>2$, g 是 p 的原根。证明：对任意正整数 k，不可能有 $g^{k+2}\equiv g^{k+1}+1\equiv g^k+2 \pmod p$ 成立。

29. 若模 m 有原根 g，则 g^k, $1\leqslant k\leqslant \phi(m)$, $(k,\phi(m))=1$ 是两两对模 m 不同余的模 m 的所有原根，个数为 $\phi(\phi(m))$。

30. 若模 m 有原根，$m\neq 3,4,6$，则模 m 的所有正原根 $g(1<g<m)$ 之积对模 m 同余于 1。

31. (i) 设素数 $p=2^n+1 (n>1)$，证明：3 是 p 的原根；

(ii) 设 $m=2^n+1 (n>1)$。证明：m 是素数的充要条件是 $3^{(m-1)/2}\equiv -1 \pmod m$。

32. 设素数 $p=2^{4n}+1$。证明：7 是 p 的原根。

§2 原 根

本节主要证明

定理1 模 m 有原根的充要条件是

$$m=1,2,4,p^\alpha,2p^\alpha,$$

其中 p 是奇素数，$\alpha\geqslant 1$。

定理的必要性已由§1性质12推出。当 $m=1,2,4$ 时原根分别

为1，1，-1。所以，定理归结为要证明 $m=p^{\alpha},2p^{\alpha}$ 时有原根。下面分两个定理来证明这一结论。

定理2 设 p 是素数，则模 p 必有原根。事实上，对每一正整数 $d|p-1$，在模 p 的一个既约剩余系中恰有 $\varphi(d)$ 个数对模 p 的指数为 d。

证法一 由§1性质11知，一定存在整数 g 使得

$$\delta_p(g)=[\delta_p(1),\delta_p(2),\cdots,\delta_p(p-1)]=\delta.$$

显见，$\delta|p-1$，及 $\delta_p(j)|\delta,j=1,2,\cdots,p-1$。因而，同余方程

$$x^{\delta}-1\equiv 0(\mathrm{mod}\ p)$$

有解 $x\equiv 1,2,\cdots,p-1(\mathrm{mod}\ p)$。由第四章§8定理2知：$p-1\leqslant\delta$。所以，$\delta=p-1$。这就说明了 g 是模 p 的原根。由此及§1性质5和7（取 $a=g$）就可推出定理的后一部分结论（留给读者）。

证法二 设 $d|p-1$，以 $\psi(d)$ 表示模 p 的一个既约剩余系中对模 p 的指数等于 d 的元素的个数，我们有

$$\sum_{d|p-1}\psi(d)=p-1. \tag{1}$$

对模 p 指数为 d 的数必满足同余方程

$$x^d-1\equiv 0(\mathrm{mod}\ p). \tag{2}$$

显然有 $x^d-1|x^p-x=x(x^{p-1}-1)$，所以由第四章§8定理5知同余方程(2)的解数为 d。如果存在 a 对模 p 的指数为 d，则由§1性质5知，(2)的全部解为

$$x\equiv a^0,a^1,\cdots,a^{d-1}(\mathrm{mod}\ p). \tag{3}$$

而由性质7知，(3)中仅有 $a^j((j,d)=1,0\leqslant j\leqslant d-1)$ 对模 p 的指数为 d，即有 $\varphi(d)$ 个数对模 p 的指数为 d。这样就证明了：

$$\psi(d)=\begin{cases}\varphi(d), & \text{存在 } a \text{ 对模 } p \text{ 的指数为 } d;\\ 0, & \text{不存在 } a \text{ 对模 } p \text{ 的指数为 } d.\end{cases} \tag{4}$$

由第三章§3定理2知

$$\sum_{d|p-1}\varphi(d)=p-1.$$

由此及式(1)得

$$\sum_{d|p-1}(\phi(d)-\psi(d))=0.$$

由此及式(4)就推出：对所有的 $d|p-1$ 必有

$$\psi(d)=\phi(d). \tag{5}$$

特别地有

$$\psi(p-1)=\phi(p-1). \tag{6}$$

这就证明了原根的存在性以及全部结论。

定理3 设 p 为奇素数。那么，对任意的 $\alpha\geqslant1$，模 p^{α} 必有原根。事实上，存在 $\bar{g}$ 使得对所有的 $\alpha\geqslant1$，$\bar{g}$ 是模 p^{α}，模 $2p^{\alpha}$ 的公共的原根。

证 分以下几步来证。

(i) 若 g 是模 $p^{\alpha+1}(\alpha\geqslant1)$ 的原根，则 g 一定是模 p^{α} 的原根。设 $\delta=\delta_{p^{\alpha}}(g)$。由§1性质3知 $\delta|\phi(p^{\alpha})$。由

$$g^{\delta}\equiv1 \pmod{p^{\alpha}}$$

可推出(为什么)

$$g^{p\delta}\equiv1 \pmod{p^{\alpha+1}}.$$

进而，从§1性质2及假设知，

$$\phi(p^{\alpha+1})=\delta_{p^{\alpha+1}}(g)|p\delta.$$

由于(见第三章§2定理8)

$$\phi(p^{k})=p^{k-1}(p-1), \qquad k\geqslant1, \tag{7}$$

从以上两式得 $\phi(p^{\alpha})|\delta$。因此 $\delta=\phi(p^{\alpha})$。这就证明了所要结论。

(ii) 若 g 是模 $p^{\alpha}(\alpha\geqslant1)$ 的原根，则必有

$$\delta_{p^{\alpha+1}}(g)=\phi(p^{\alpha}) \text{ 或 } \phi(p^{\alpha+1}).$$

因由假设及§1性质9(i)知，$\phi(p^{\alpha})=\delta_{p^{\alpha}}(g)|\delta_{p^{\alpha+1}}(g)$。而由§1性质3知 $\delta_{p^{\alpha+1}}(g)|\phi(p^{\alpha+1})$。由此利用式(7)就推出所要结论。

(iii) 当 p 为奇素数时，若 g 是模 p 的原根，且有

$$g^{p-1}=1+rp, \qquad p\nmid r, \tag{8}$$

则 g 是所有模 $p^\alpha(\alpha\geqslant 1)$ 的原根。我们来证明：对 $\alpha\geqslant 1$ 有

$$g^{\phi(p^\alpha)}=1+r(\alpha)p^\alpha,\qquad p\nmid r(\alpha),\tag{9}$$

其中 $r(\alpha)$ 是一整数。当 $\alpha=1$ 时，式(9)就是式(8)，所以成立。设式(9)对 $\alpha=n(\geqslant 1)$ 成立。当 $\alpha=n+1$ 时，由归纳假设得

$$\begin{aligned}g^{\phi(p^{n+1})}&=(1+r(n)p^n)^p\\&=1+r(n)p^{n+1}+\frac{1}{2}p(p-1)r^2(n)p^{2n}+\cdots\\&=1+r(n+1)p^{n+1},\end{aligned}$$

这里

$$r(n+1)\equiv r(n)+\frac{1}{2}(p-1)r^2(n)p^n\pmod p.$$

由于 p 是奇数及 $p\nmid r(n)$，所以 $p\nmid r(n+1)$。这就证明了式(9)对 $\alpha=n+1$ 成立。因此，式(9)对任意的 $\alpha\geqslant 1$ 都成立。由式(9)及(ii)就推出 g 是所有模 p^α 的原根。

(iv) 设 p 为奇素数，g' 是模 p 的原根且为奇数(若 g' 是偶数则以 $g'+p$ 代 g')。那么，

$$g=g'+tp,\qquad t=0,1,\cdots,p-1,\tag{10}$$

都是模 p 的原根，且除了一个以外，都满足条件(8)。我们有

$$g^{p-1}=(g'+tp)^{p-1}=(g')^{p-1}+(p-1)(g')^{p-2}pt+Ap^2,$$

其中 A 为整数。设 $(g')^{p-1}=1+ap$，由上式得

$$g^{p-1}=1+((p-1)(g')^{p-2}t+a)p+Ap^2.$$

由于 $(p,(p-1)g')=1$，所以，t 的一次同余方程

$$(p-1)(g')^{p-2}t+a\equiv 0\pmod p$$

的解数为 1(第四章 §2定理1)。这就证明了所要的结论。由于 $t=0,1,\cdots,p-1$ 中至少有两个偶数及 g' 为奇，所以，总可取到模 p 的一个原根 g 为奇数且满足条件(8)。我们把它记为 $\bar{g}$。

(v) 由(iii)和(iv)立即推出 $\bar{g}$ 是所有模 $p^\alpha(\alpha\geqslant 1)$ 的原根。由于 $\bar{g}$ 为奇数，所以

$$(\bar{g})^d \equiv 1 \pmod{p^\alpha}$$

与

$$(\bar{g})^d \equiv 1 \pmod{2p^\alpha}$$

等价。因此 $\delta_{2p^\alpha}(\bar{g}) = \delta_{p^\alpha}(\bar{g}) = \varphi(p^\alpha)$，由此及 $\varphi(2p^\alpha) = \varphi(p^\alpha)$ 就推出 $\bar{g}$ 是所有模 $2p^\alpha(\alpha \geqslant 1)$ 的原根。证毕。

由§1性质12及定理2、定理3就完全证明了定理1。如何求原根是一个很困难的问题。首先要去求模 p 的原根，然后依照定理3的证明中的方法去求模 p^α 及 $2p^\alpha$ 的原根。但求模 p 的原根没有一般的方法，只能对具体的素数 p 按原根的定义逐个数去试算。下面来举几个例。

例1　求 $p = 23$ 的原根。

解　由于 a 对模 p 的指数必是 $p-1$ 的除数，所以为求出指数只要去计算 a^d 对模 p 的剩余，$d \mid p-1$。

这里 $p-1 = 22 = 2 \cdot 11$，它的除数 $d = 1, 2, 11, 22$。先求 $a = 2$ 对模23的指数：

$$2^2 \equiv 4 \pmod{23},$$

$$2^{11} \equiv (2^4)^2 \cdot 2^3 \equiv (-7)^2 \cdot 8 \equiv 3 \cdot 8 \equiv 1 \pmod{23}.$$

所以 $\delta_{23}(2) = 11$，2不是模23的原根。再求 $a = 3$ 对模23的指数：

$$3^2 \equiv 9 \pmod{23}, \qquad 3^3 \equiv 4 \pmod{23},$$

$$3^{11} \equiv (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \pmod{23}.$$

所以，$\delta_{23}(3) = 11$，3不是模23的原根。再求 $\delta_{23}(4)$。

$$4^2 \equiv -7 \pmod{23}, \qquad 4^{11} \equiv (4^4)^2 \cdot 4^3 \equiv 3^2 \cdot (-5) \equiv 1 \pmod{23}.$$

所以 $\delta_{23}(4) = 11$，4不是模23的原根。再求 $\delta_{23}(5)$。

$$5^2 \equiv 2 \pmod{23},$$

$$5^{11} \equiv (5^4)^2 \cdot 5^3 \equiv 4^2 \cdot 10$$

$$\equiv 4 \cdot (-6) \equiv -1 \pmod{23}.$$

$$5^{22} \equiv 1 \pmod{23}.$$

所以，$\delta_{23}(5) = 22$，5是模23的原根，且是最小正原根。

为了进一步求出模 p^α，$2p^\alpha$ 的原根，就要验证式(8)当 $g = 5$，

$p=23$时是否成立。这实际上就是求g^{p-1}对模p^2的剩余。这里$23^2=529$。

$5^2\equiv25\pmod{23^2}$,

$5^8\equiv(23+2)^4\equiv4\cdot23\cdot2^3+2^4\equiv10\cdot23-7\pmod{23^2}$,

$5^{10}\equiv(10\cdot23-7)(23+2)\equiv13\cdot23-14$

$\equiv12\cdot23+9\pmod{23^2}$,

$5^{20}\equiv(12\cdot23+9)^2\equiv216\cdot23+81\equiv13\cdot23-11\pmod{23^2}$,

$5^{22}\equiv(13\cdot23-11)(23+2)\equiv15\cdot23-22$

$\equiv1+14\cdot23\pmod{23^2}$。

由$23\nmid14$及5是奇数就证明了5是所有模23^α, $2\cdot23^\alpha$的原根。

例2　求模41的原根。

解　$41-1=40=2^3\cdot5$，除数$d=1,2,4,8,5,10,20,40$。依次来求$a=2,3,\cdots$的指数。

$2^2\equiv4\pmod{41}$, $2^4\equiv16\pmod{41}$, $2^5\equiv-9\pmod{41}$,

$2^{10}\equiv-1\pmod{41}$, $2^{20}\equiv1\pmod{41}$.

所以$\delta_{41}(2)\mid20$，由于$d\mid20$，$d<20$时，$2^d\not\equiv1\pmod{41}$，所以，$\delta_{41}(2)=20$。2不是原根。

$3^2\equiv9\pmod{41}$,　　$3^4\equiv-1\pmod{81}$,　　$3^8\equiv1\pmod{41}$.

同理可得$\delta_{41}(3)=8$。所以3也不是原根。

注意到$[\delta_{41}(2),\delta_{41}(3)]=[20,8]=40$。所以我们不用依次计算$4,5,\cdots$的指数，而可利用§1性质11来求原根，注意到

$$\delta_{41}(2)=4\cdot5,\quad \delta_{41}(3)=1\cdot8.$$

由性质11知$c=2^4\cdot3=48$是原根。因此，7也是模41的原根。这一求原根的方法实质上就是定理2的证法一，因此证法一在某些情形下是寻找原根的一种方法。

为求41^α，$2\cdot41^\alpha$的原根要计算7^{40}对模$41^2=1681$的剩余。

$$7^2\equiv41+8\pmod{41^2},$$

$$7^4\equiv(41+8)^2\equiv18(41-1)\pmod{41^2},$$

$$7^5\equiv3\cdot(41+1)(41-1)\equiv-3\pmod{41^2},$$

$$7^{10}\equiv 9(\bmod 41^2),\qquad 7^{20}\equiv 81(\bmod 41)^2,$$

$$7^{40}\equiv(2\cdot 41-1)^2\equiv 1+(-4)\cdot 41(\bmod 41^2).$$

由$41\nmid -4$，7是奇数，就推出7是所有模41^α，$2\cdot 41^\alpha$的原根．

例3 求模43的原根。

解 $43-1=42=2\cdot 3\cdot 7$．除数$d=1,2,3,7,6,14,21,42$．先求2的指数．

$$2^2\equiv 4(\bmod 43),\qquad 2^3\equiv 8(\bmod 43),\qquad 2^6\equiv 8^2\equiv 21(\bmod 43),$$

$$2^7\equiv -1(\bmod 43),\qquad 2^{14}\equiv 1(\bmod 43).$$

所以，$\delta_{43}(2)=14$．再求3的指数．

$$3^2\equiv 9(\bmod 43),\qquad 3^3\equiv -16(\bmod 43),$$

$$3^4\equiv -5(\bmod 43),\qquad 3^6\equiv 9\cdot(-5)\equiv -2(\bmod 43),$$

$$3^7\equiv -6(\bmod 43),\qquad 3^{14}\equiv 36\equiv -7(\bmod 43),$$

$$3^{21}\equiv -1(\bmod 43).$$

所以3是模43的原根．

下面来求3^{42}对模$43^2=1849$的剩余，

$$3^4\equiv 81\equiv 2\cdot 43-5(\bmod 43^2),$$

$$3^8\equiv(2\cdot 43-5)^2\equiv -5(4\cdot 43-5)(\bmod 43^2),$$

$$3^{16}\equiv 5^2(3\cdot 43+25)(\bmod 43^2),$$

$$3^{20}\equiv 5^2(3\cdot 43+25)(2\cdot 43-5)\equiv 5^2(35\cdot 43-125),$$

$$\equiv -5^2(11\cdot 43-4).$$

$$3^{21}\equiv -(2\cdot 43-11)(11\cdot 43-4)\equiv -44(\bmod 43^2),$$

$$3^{42}\equiv(43+1)^2\equiv 1+2\cdot 43(\bmod 43^2).$$

由$43\nmid 2$及3为奇数知3是所有模43^α，$2\cdot 43^\alpha$的原根．

例1和例3中求模p的原根的方法，是对所有$p-1$的除数d，$d<p-1$计算了a^d对模p的剩余，当这些剩余都不等于1时，就证明了a是模p的原根．这个方法稍加修改就可表述为下面的定理(证明留给读者)．

定理4 设p是奇素数，$p-1$的所有的不同的素因数是$q_1,\cdots,q_s$．那么，g是模p的原根的充要条件是

$$g^{(p-1)/q_j} \not\equiv 1 \pmod p, \quad j=1,\cdots,s. \tag{11}$$

显见，定理4把p改为任意正整数$m\geqslant 2$，$p-1$改为$\phi(m)$定理仍然成立，但实质上用具体数值验证式(11)并不比验证$p-1$的所有正除数$d<p-1$方便多少。请读者自己用定理4的方法来做例2，例3，并比较之。

由定理1及第三章§3定理4立即推出：

定理5 设$m\geqslant 1$。模m的既约剩余系能表为：

$$g^0, g^1, \cdots, g^{\phi(m)-1}, \tag{12}$$

这里g为某一整数，当且仅当$m=1,2,4,p^\alpha,2p^\alpha$（$p$奇素数，$\alpha\geqslant 1$），即模$m$有原根。

事实上，第三章§3定理4就是证明了模m有形如(12)的既约剩余系的充要条件是模m有原根。由此及定理1就完全证明了定理5。

形式(12)给出了既约剩余系的一个十分便于研究的形式，虽然这一点对大部分合数模都不成立，但合数模的既约剩余系可以通过若干个素数幂模的既约剩余系来构造（见第三章§2，§3），这些我们将在下节讨论。

习　题　二

1．试求模11,13,17,19,31,37,53,71的最小正原根。

2．试求一个g，它是模p的原根，但不是模p^2的原根：$p=5,7,11,17,31$。

3．证明10是487的原根，但不是487^2的原根。

4．试求一个g，对所有的$\alpha\geqslant 1$，它是p^α，$2p^\alpha$的原根：

$$p=11,13,17,19,31,37,53,71.$$

5．设p是素数，$k\geqslant 1$。证明

$$1^k+2^k+\cdots+(p-1)^k \equiv \begin{cases} 0 \pmod p, & p-1\nmid k, \\ -1 \pmod p, & p-1\mid k. \end{cases}$$

6．设素数$p>2$，$p-1$的标准素因数分解式是$q_1^{\beta_1}\cdots q_r^{\beta_r}$。

证明：

(i) 对任一 $j(1\leqslant j\leqslant r)$，存在 a_j 对模 p 的指数是 $q_j^{\beta_j}$（不能利用模 p 存在原根）；

(ii) $a_1\cdots a_r$ 是模 p 的原根；

(iii) 举例说明如何用这一方法来构造模23的原根。

7. 设$1975\leqslant n\leqslant 1985$，问其中哪些 n 有原根。

8. 求以10为原根的最小素数。

9. 求模 p^2 的所有原根 g，$1<g<p$；$p=19,31,37,53,71$。

10. 求模$2p$的所有原根 g，$1<g<2p$；$p=19,31,37,53,71$。

11. 设 $\lambda(m)$ 由 §1 式（7）给出。证明：一定存在 a，使 $\delta_m(a)=\lambda(m)$，且至少有$\phi(\lambda(m))$个两两对模 m 不同余的 a 有这性质。

§3 指标、指标组与既约剩余系的构造

第三章§3定理 4（或上节定理 5）证明了：当模 m 有原根 g 时，它的既约剩余系可表为

$$g^0=1,g^1,\cdots,g^{\phi(m)-1}. \tag{1}$$

也就是说，对任一 $a,(a,m)=1$，必可唯一地表为：

$$a\equiv g^{\gamma}\pmod m,\qquad 0\leqslant\gamma<\phi(m). \tag{2}$$

这表明当 m 有原根时，通过原根 g，模 m 的既约剩余系与模$\phi(m)$的完全剩余系之间可建立一一对应的关系，这种对应由式(2)给出。第三章§3定理5证明了：当 $\delta_{2^\alpha}(g_0)=2^{\alpha-2}$ 时，模 $m=2^\alpha(\alpha\geqslant 3)$的既约剩余系可表为：

$$\pm g_0^0=\pm 1,\pm g_0^1,\cdots,\pm g_0^{2^{\alpha-2}-1}. \tag{3}$$

也就是说，对任一 a，$(a,2)=1$，必可唯一地表为：

$$a\equiv(-1)^{\gamma^{(-1)}}g_0^{\gamma^{(0)}}\pmod{2^\alpha}, \tag{4}$$

$$0\leqslant\gamma^{(-1)}<2,\qquad 0\leqslant\gamma^{(0)}<2^{\alpha-2}.$$

这表明模 $2^\alpha(\alpha\geqslant3)$ 的既约剩余系，通过 -1 和 g_0，同模 2 的完全剩余系和模 $2^{\alpha-2}$ 的完全剩余系构成的数对 $\{\gamma^{(-1)},\gamma^{(0)}\}$ 之间可建立一一对应的关系，这种对应由式(4)给出。这类表示形式的优点在于：就对模 m 既约的数来说，它们对模 m 的乘法运算可转化为方幂数的加法运算。所以，这种表示形式在理论与应用上都是有用的。为此就要研究这种表示形式的基本性质。

定义1 设模 m 有原根 g，$(a,m)=1$。我们把表示式(2)中的 γ 称为是 a 对模 m 的以 g 为底的指标，记作 $\gamma_{m,g}(a)$，当不会混淆时简记作 $\gamma_g(a)$ 或 $\gamma(a)$。

定义2 设 $\alpha\geqslant3$，$(a,2)=1$。我们把表示式(4)中的 $\gamma^{(-1)}$，$\gamma^{(0)}$ 称为是 a 对模 2^α 的以 $-1,g_0$ 为底的指标组，记作 $\gamma^{(-1)}_{\alpha;-1,g_0}(a)$，$\gamma^{(0)}_{\alpha;-1,g_0}(a)$，当不会混淆时简记作

$$\gamma^{(-1)}_{g_0}(a),\quad \gamma^{(0)}_{g_0}(a) \text{ 或 } \gamma^{(-1)}(a),\quad \gamma^{(0)}(a).$$

下面分别来讨论指标与指标组的性质，实际上它们是§1关于指数性质的简单推论，只要注意到模 m 的原根对模 m 的指数为 $\phi(m)$ 以及 g_0 对模 $2^\alpha(\alpha\geqslant3)$ 的指数为 $2^{\alpha-2}$。

关于指标 $\gamma_{m,g}(a)$ 有以下性质。

性质1 设 g 是模 m 的原根，$(a,m)=1$。若

$$g^h\equiv a \pmod m,$$

则有 $h\equiv\gamma_{m,g}(a) \pmod{\phi(m)}$，且反过来也成立。

这由指标 $\gamma(a)$ 的定义、$\delta_m(g)=\phi(m)$ 及§1性质4推出。

性质2 设 g 是模 m 的原根，$(ab,m)=1$，则有

$$\gamma_{m,g}(ab)\equiv\gamma_{m,g}(a)+\gamma_{m,g}(b) \pmod{\phi(m)}. \tag{5}$$

证 记 $\gamma(c)=\gamma_{m,g}(c)$。我们有

$$ab\equiv g^{\gamma(a)}\cdot g^{\gamma(b)}\equiv g^{\gamma(a)+\gamma(b)} \pmod m.$$

由此及性质1即得所要结论。

性质3 设 $g,\bar g$ 是模 m 的两个不同的原根，$(a,m)=1$。我们有

$$\gamma_{m,\tilde{g}}(a) \equiv \gamma_{m,\tilde{g}}(g) \cdot \gamma_{m,g}(a) \pmod{\phi(m)}. \tag{6}$$

证　由

$$a \equiv g^{\gamma_{m,g}(a)} \pmod{m},$$

及

$$g \equiv \tilde{g}^{\gamma_{m,\tilde{g}}(g)} \pmod{m},$$

$$a \equiv \tilde{g}^{\gamma_{m,\tilde{g}}(a)} \pmod{m},$$

可得

$$a \equiv \tilde{g}^{\gamma_{m,\tilde{g}}(g) \cdot \gamma_{m,g}(a)} \pmod{m}.$$

由此及性质 1 即得式(6)。

特别的，在式(6)中取 $a=\tilde{g}$，即得

$$\gamma_{m,g}(g) \cdot \gamma_{m,g}(\tilde{g}) \equiv 1 \pmod{\phi(m)}. \tag{7}$$

性质 3 刻画了对不同原根的指标之间的关系。以上性质表明：通常对数的运算规则、对指标的运算（在模 $\phi(m)$ 的意义下）也成立。式（6）就相当于对数的换底公式。关于指标与指数的关系有下面的结论。

性质4　设 g 是模 m 的原根，$(a,m)=1$。我们有

$$\delta_m(a) = \phi(m)/(\gamma_{m,g}(a), \phi(m)). \tag{8}$$

由此推出，当 m 有原根时，对每个正除数 $d \mid \phi(m)$，在模 m 的一个既约剩余系中，恰有 $\phi(d)$ 个元素对模 m 的指数等于 d。特别地，恰有 $\phi(\phi(m))$ 的原根。

证　在§1性质 7 中取 $a=g$ 及 $k=\gamma_{m,g}(a)$，由 $\delta_m(g)=\phi(m)$、§1式(3)及§1性质 1 即得式(8)。当模 m 有原根时我们取由式(1)给出的既约剩余系，由式(8)知，这个既约剩余系中的元素 g^j 的指数 $\delta_m(g^j)=d$ 的充要条件是（注意 $\gamma_{m,g}(g^j)=j$，$0 \leqslant j < \phi(m)$）：

$$(\phi(m), j) = \phi(m)/d, \qquad 0 \leqslant j < m.$$

设 $j = t \cdot \phi(m)/d$，上式等价于

$$(d,t)=1, \qquad 0 \leqslant t < d.$$

满足上式的 t 恰有 $\phi(d)$ 个。这就证明了所要的结论。

性质 4 的证明表明了有形如（1）的既约剩余系的优点。由性质 4 的证明知，当模 m 有原根时，对任一 $d\mid\phi(m)$，指数为 d 的 $\phi(d)$ 个数是

$$g^{t\phi(m)/d},\quad 0\leqslant t<d,\ (t,d)=1. \tag{9}$$

特别地，$\phi(\phi(m))$ 个原根是

$$g^{t},\quad 0\leqslant t<\phi(m),\ (t,\phi(m))=1. \tag{10}$$

当已知模 m 的一个原根 g 时，我们通过依次计算式(1)中的 g^{j} $(0\leqslant j<\phi(m))$ 对模 m 的绝对最小剩余或最小正剩余，就可得到模 m 的绝对最小既约剩余系或最小既约正剩余系的每个元素的指标，由此从式（8）得到指数。把所得这些结果，按指标的大小顺序或既约剩余系的大小顺序来列表。这种表(通常称为**指标表**)可供具体应用时查用，是十分方便的。下面来举几个例。

例 1 构造模23以原根 5 为底的指标表。

由 § 2 例1知，5 是模23的原根，$\phi(23)=22$。先按指标的次序来列表 1，因为依次计算5^{j}对模23的绝对最小剩余比较容易。

表 1

$\gamma_{23,5}(a)$	0	1	2	3	4	5	6	7	8	9	10
a	1	5	2	10	4	−3	8	−6	7	11	9
$\delta_{23}(a)$	1	22	11	22	11	22	11	22	11	22	11
$\gamma_{23,5}(a)$	11	12	13	14	15	16	17	18	19	20	21
a	−1	−5	−2	−10	−4	3	−8	6	7	−11	−9
$\delta_{23}(a)$	2	11	22	11	22	11	22	11	22	11	22

按照绝对最小既约剩余系的大小次序来排，指标表1就变为表 2。

表 2

a	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
$\gamma_{23,5}(a)$	20	14	21	17	8	7	12	15	5	13	11
$\delta_{23}(a)$	11	11	22	22	11	22	11	22	22	22	2

a	1	2	3	4	5	6	7	8	9	10	11
$\gamma_{23,5}(a)$	0	2	16	4	1	18	19	6	10	3	9
$\delta_{23}(a)$	1	11	11	11	22	11	22	11	11	22	22

由表知，模23的原根（即指数等于22的元素）有10个，它们是：

$$-9,-8,-6,-4,-3,-2,5,7,10,11. \qquad (11)$$

指数为11的元素有10个，它们是：

$$-11,-10,-7,-5,2,3,4,6,8,9. \qquad (12)$$

指数为 2 的元素有一个：-1。指数为 1 的有一个：1。

关于模 $m=2^\alpha\,(\alpha\geqslant 3)$ 的指标组 $\gamma^{(-1)}_{\alpha;-1,g_0}(a)$，$\gamma^{(0)}_{\alpha;-1,g_0}(a)$，我们仅讨论 $g_0=5$ 的情形，并把它们简记作 $\gamma^{(-1)}(a)$，$\gamma^{(0)}(a)$。

性质5 若 $a\equiv(-1)^j 5^h \pmod{2^\alpha}$，则有

$$j\equiv\gamma^{(-1)}(a)\equiv(a-1)/2 \pmod 2, \qquad (13)$$

及

$$h\equiv\gamma^{(0)}(a) \pmod{2^{\alpha-2}}. \qquad (14)$$

证 由条件及式(4)($g_0=5$)得

$$a\equiv(-1)^j\equiv(-1)^{\gamma^{(-1)}(a)} \pmod 4,$$

由此即得式(13)。由条件，式(4)($g_0=5$)，及式(13)得：

$$5^h\equiv 5^{\gamma^{(0)}(a)} \pmod{2^\alpha}.$$

由于 $\delta_{2^\alpha}(5)=2^{\alpha-2}$，由上式及§1性质 4 就推出式(14)。

性质6 设 $(ab,2)=1$。我们有

$$\gamma^{(-1)}(ab)\equiv\gamma^{(-1)}(a)+\gamma^{(-1)}(b)\pmod 2, \qquad (15)$$

及

$$\gamma^{(0)}(ab)\equiv\gamma^{(0)}(a)+\gamma^{(0)}(b)\pmod{2^{\alpha-2}}. \qquad (16)$$

证 由式(4)得

$$ab\equiv(-1)^{\gamma^{(-1)}(a)+\gamma^{(-1)}(b)}5^{\gamma^{(0)}(a)+\gamma^{(0)}(b)}\pmod{2^\alpha}.$$

由此及性质 5 即得所要结论。

性质7 设$(a,2)=1$。我们有

$$\delta_{2^\alpha}(a)=\begin{cases}2^{\alpha-2}/(\gamma^{(0)}(a),2^{\alpha-2}), & 0<\gamma^{(0)}(a)<2^{\alpha-2},\\ 2/(\gamma^{(-1)}(a),2), & \gamma^{(0)}(a)=0.\end{cases} \qquad (17)$$

证 $\gamma^{(0)}(a)=0$的充要条件是$a\equiv(-1)^{\gamma^{(-1)}(a)}\equiv\pm1\pmod{2^\alpha}$，容易直接验证这时式(17)成立，当 $0<\gamma^{(0)}(a)<2^{\alpha-2}$ 时，一定有$a\not\equiv1\pmod{2^\alpha}$，所以$2|\delta_{2^\alpha}(a)$(为什么)。设$b=5^{\gamma^{(0)}(a)}$。以下记$\delta(a)=\delta_{2^\alpha}(a),\delta(b)=\delta_{2^\alpha}(b)$。由§1性质 7 得(注意$\delta(5)=2^{\alpha-2}$)：

$$\delta(b)=2^{\alpha-2}/(\gamma^{(0)}(a),2^{\alpha-2}). \qquad (18)$$

由$0<\delta^{(0)}(a)<2^{\alpha-2}$知$2|\delta(b)$。由$2|\delta(a)$推出。

$$1\equiv a^{\delta(a)}\equiv((-1)^{\gamma^{(-1)}(a)}b)^{\delta(a)}\equiv b^{\delta(a)}\pmod{2^\alpha}.$$

由$2|\delta(b)$推出

$$a^{\delta(b)}\equiv((-1)^{\gamma^{(-1)}(a)}b)^{\delta(b)}\equiv b^{\delta(b)}\equiv1\pmod{2^\alpha}.$$

利用§1性质 2，由以上两式分别推出$\delta(b)|\delta(a)$ 及 $\delta(a)|\delta(b)$。因此有$\delta(a)=\delta(b)$，进而由式(18)推出这时式(17)也成立。证毕。

由性质 7 推出：

性质8 设$\alpha\geqslant3$。$1\leqslant d|2^{\alpha-2}$，及以$\psi(d)$记在模 2^α 的一个既约剩余系中指数为d的元素个数。我们有

$$\psi(d)=\begin{cases}1, & d=1,\\ 3, & d=2,\\ 2\phi(d), & 2<d|2^{\alpha-2}.\end{cases} \qquad (19)$$

证 我们取式(4)($g_0=5$)给出的模2^α的既约剩余系。由式(17)知，$\delta_{2^\alpha}(a)=1$的充要条件是$\gamma^{(0)}(a)=\gamma^{(-1)}(a)=0$，即

$a\equiv 1 \pmod{2^\alpha}$。所以式(19)成立。由式(17)知，$\delta_{2^\alpha}(a)=2$ 的充要条件是 $\gamma^{(0)}(a)=0$，$\gamma^{(-1)}(a)=1$；或 $\gamma^{(0)}(a)=2^{\alpha-3}$，$\gamma^{(-1)}(a)=0,1$，所以在一个既约剩余系中这样的元素有三个，因此式(19)也成立。当 $d>2$，$d|2^{\alpha-2}$ 时，可设 $d=2^j$，$1<j\leqslant 2^{\alpha-2}$。由式(17)知，$\delta_{2^\alpha}(a)=d=2^j$ 的充要条件是：

$$(\gamma^{(0)}(a),2^{\alpha-2})=2^{\alpha-2-j},\qquad 0\leqslant\gamma^{(0)}(a)<2^{\alpha-2}.$$

设 $\gamma^{(0)}(a)=2^{\alpha-2-j}\cdot t$，上式即

$$(t,2^j)=1,\qquad 0\leqslant t<2^j.$$

这样的 t 有 $\phi(2^j)=\phi(d)$ 个，由此及 $\gamma^{(-1)}(a)$ 可取0，1两个值，所以，在一个既约剩余系中指数为 d $(2<d|2^{\alpha-2})$ 的元素恰有 $2\phi(d)$ 个。

类似于有原根时模 m 的指标表，我们可以来列出模2^α $(\alpha\geqslant 3)$ 的指标组表，其中的指数 $\delta(a)=\delta_{2^\alpha}(a)$ 由式(17)推出。

例 2 构造模 $2^6=64$ 的指标组表（$\alpha=6$）。

表 3

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	5	25	−3	−15	−11	9	−19	−31	−27	−7	29	17	21	−23	13
$\delta(a)$	1	2^4	2^3	2^4	2^2	2^4	2^3	2^4	2	2^4	2^3	2^4	2^2	2^4	2^3	2^4

续表3

$\gamma^{(-1)}(a)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	−1	−5	−25	3	15	11	−9	19	31	27	7	−29	−17	−21	23	−13
$\delta(a)$	2	2^4	2^3	2^4	2^2	2^4	2^3	2^4	2	2^4	2^3	2^4	2^2	2^4	2^3	2^4

表3是按照指标 $\gamma^{(0)}(a)$ 的大小次序，分别 $\gamma^{(-1)}(a)=0$、$\gamma^{(-1)}(a)=1$ 来排列的。由此可得到按模 2^6 的绝对最小剩余系排列的指标

表（见表4）。

表 4

$\gamma^{(-1)}(a)$	0	1	0	1	0	1	0	1
$\gamma^{(0)}(a)$	8	11	9	2	14	13	7	12
a	-31	-29	-27	-25	-23	-21	-19	-17
$\delta(a)$	2	2^4	2^4	2^3	2^3	2^4	2^4	2^2

续表4

$\gamma^{(-1)}(a)$	0	1	0	1	0	1	0	1
$\gamma^{(0)}(a)$	4	15	5	6	10	1	3	0
a	-15	-13	-11	-9	-7	-5	-3	-1
$\delta(a)$	2^2	2^4	2^4	2^3	2^3	2^4	2^4	2

续表4

$\gamma^{(-1)}(a)$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\gamma^{(0)}(a)$	0	3	1	10	6	5	15	4	12	7	13	14	2	9	11	8
a	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
$\delta(a)$	1	2^4	2^4	2^3	2^3	2^4	2^4	2^2	2^2	2^4	2^4	2^3	2^3	2^4	2^4	2

当 $\alpha\leqslant2$ 时，模 2^α 有原根，它的既约剩余系可由式(1)的形式给出；当 $\alpha\geqslant3$ 时，模 2^α 没有原根；它的既约剩余系可由式(4)（我们总取定 $g_0=5$）给出。为了叙述方便，我们把这两种情形统一起来。设

$$c_{-1}(\alpha)=c_{-1}=\begin{cases}1, & \alpha=1,\\ 2, & \alpha\geqslant2;\end{cases}\qquad c_0(\alpha)=c_0=\begin{cases}1, & \alpha=1,\\ 2^{\alpha-2}, & \alpha\geqslant2.\end{cases}\tag{20}$$

那么，当 $\alpha\geqslant1$ 时，

$$(-1)^{\gamma^{(-1)}}5^{\gamma^{(0)}},\qquad 0\leqslant\gamma^{(-1)}<c_{-1},\ 0\leqslant\gamma^{(0)}<c_0\tag{21}$$

是模 2^α 的一组既约剩余系。这一结论对 $\alpha=1,2$ 很容易直接验证，当 $\alpha\geqslant3$ 时，这就是式(3)（$g_0=5$）。无论何种情形，当

$$a \equiv (-1)^{\gamma^{(-1)}} 5^{\gamma^{(0)}} \pmod{2^{\alpha}}$$

时，我们都把$\{\gamma^{(-1)}, \gamma^{(0)}\}$称为对模 2^{α} 的指标组。显见，$a=1, 2$时必有 $\gamma^{(0)}=0$。

至此，我们讨论了模 p^{α} 的既约剩余系的形如(1)或(3)的构造形式，以及每一$a((a,p^{\alpha})=1)$必唯一对应于一个指标，或指标组(见式(2)或(4))。利用第四章§3定理1(即孙子定理)，由此就可得到对任意模 m 的相应结果。

定理1 设 $p_j (1 \leqslant j \leqslant r)$是不同的奇素数，$\alpha_j \geqslant 1 (1 \leqslant j \leqslant r)$，

$$m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \tag{22}$$

$c_{-1} = c_{-1}(\alpha_0)$，$c_0 = c_0(\alpha_0)$由式(20)给出，

$$c_j = c_j(p_j^{\alpha_j}) = \phi(p_j^{\alpha_j}), \quad 1 \leqslant j \leqslant r. \tag{23}$$

再设 $m = M_0 2^{\alpha_0}$，$m = M_j p_j^{\alpha_j}$ $(1 \leqslant j \leqslant r)$，$M_j^{-1}$ $(0 \leqslant j \leqslant r)$为取定的一组整数，满足（记 $p_0 = 2$）

$$M_j M_j^{-1} \equiv 1 \pmod{p_j^{\alpha_j}}, \quad 0 \leqslant j \leqslant r. \tag{24}$$

再设 g_j 是模 $p_j^{\alpha_j}$ 的原根$(1 \leqslant j \leqslant r)$，那么，

$$\left\{\begin{array}{ll} x = M_0 M_0^{-1} (-1)^{\gamma^{(-1)}} 5^{\gamma^{(0)}} + M_1 M_1^{-1} g_1^{\gamma^{(1)}} + \cdots + M_r M_r^{-1} g_r^{\gamma^{(r)}}, & (25) \\ 0 \leqslant \gamma^{(j)} < c_j, \quad -1 \leqslant j \leqslant r & (26) \end{array}\right.$$

就给出了模 m 的一组既约剩余系。当 $\alpha_0 = 0$时，以上式子中不出现 c_{-1}, c_0 及 $j=0$ 的项。

由式(24)及 M_j 的定义知

$$x \equiv (-1)^{\gamma^{(-1)}} 5^{\gamma^{(0)}} \pmod{2^{\alpha_0}},$$

$$x \equiv g_j^{\gamma^{(j)}} \pmod{p_j^{\alpha_j}}, \quad 1 \leqslant j \leqslant r.$$

所以，$\gamma^{(-1)}, \gamma^{(0)}$是 x 对模 2^{α} 的指标组，$\gamma^{(j)} (1 \leqslant j \leqslant r)$是 x 对模 $p_j^{\alpha_j}$的指标。此外，由定理1知，对任一$a, (a,m)=1$，必有唯一的一组满足条件(26)的 $\gamma^{(j)} = \gamma^{(j)}(a)$ $(-1 \leqslant j \leqslant r)$，使得

$$a \equiv M_0 M_0^{-1}(-1)^{\gamma^{(-1)}} 5^{\gamma^{(0)}} + M_1 M_1^{-1} g_1^{\gamma^{(1)}} + \cdots + M_r M_r^{-1} g_r^{\gamma^{(r)}} \pmod m. \tag{27}$$

这样，我们就可对任意模 m 引进指标组的概念。

定义3 设 $m>1$ 由式(22)给出，$(a,m)=1$。我们把使式(27)成立的 $\gamma^{(-1)}(a),\gamma^{(0)}(a);\gamma^{(1)}(a),\cdots,\gamma^{(r)}(a)$ 称为是 a 对模 m 的以 $-1,5;g_1,\cdots,g_r$ 为底的**指标组**。记作 $\gamma_m(a)=\{\gamma^{(-1)}(a),\gamma^{(0)}(a);\gamma^{(1)}(a),\cdots,\gamma^{(r)}(a)\}$。

对于取定的 $-1,5$ 及原根 $g_1,\cdots,g_r$，指标组显然具有以下性质（请读者自证，符号同定理 1）：

性质9 $\gamma_m(a)=\{\gamma^{(-1)},\gamma^{(0)};\gamma^{(1)},\cdots,\gamma^{(r)}\}$ 的充要条件是：$\gamma^{(-1)}$，$\gamma^{(0)}$ 是 a 对模 $2^{\alpha}c$ 的指标组，$\gamma^{(j)}$ 是 a 对模 $p_j^{\alpha_j}$ 的指标，以及 a 遍历模 m 的既剩余系的充要条件是 $\gamma^{(j)}$ 分别遍历模 c_j 的完全剩余系，$-1\leqslant j\leqslant r$。

性质10 若

$$a \equiv M_0 M_0^{-1}(-1)^{h^{(-1)}} 5^{h^{(0)}} + M_1 M_1^{-1} g_1^{h^{(1)}} + \cdots + M_r M_r^{-1} g_r^{h^{(r)}} \pmod m,$$

则有 $h^{(j)}=\gamma^{(j)}(a) \pmod{c_j}$，$-1\leqslant j\leqslant r$。

性质11 若 $(ab,m)=1$，则

$$\gamma^{(j)}(ab) \equiv \gamma^{(j)}(a)+\gamma^{(j)}(b) \pmod{c_j}, \qquad -1\leqslant j\leqslant r.$$

由式(25)给出的模 m 的既约剩余系，在应用中是完全足够了。但有一点不足的地方是：在式(25)中出现了加法，及 M_j，M_j^{-1}，不像式(1)，式(3)那样，完全由若干个元素的乘幂给出。这是容易弥补的。

定理2 在定理 1 的符号下，设

$$\bar{g}_l = M_0 M_0^{-1}(-1)^{h_l^{(-1)}} 5^{h_l^{(0)}} + M_1 M_1^{-1} g_1^{h_l^{(1)}} + \cdots + M_r M_r^{-1} g_r^{h_l^{(r)}}, \quad -1\leqslant l\leqslant r, \tag{28}$$

其中取定

$$h_l^{(l)}=1, \qquad h_l^{(j)}=0, \qquad j\neq l, \quad -1\leqslant j\leqslant r. \tag{29}$$

那么，以下 $\varphi(m)$ 个数就给出了模 m 的一组既约剩余系：

$$\begin{cases} x=\tilde{g}_{-1}^{\gamma^{(-1)}}\ \tilde{g}_0^{\gamma^{(0)}}\ \tilde{g}_1^{\gamma^{(1)}}\cdots\tilde{g}_r^{\gamma^{(r)}}, \\ 0\leqslant\gamma^{(j)}<c_j,\quad -1\leqslant j<r. \end{cases} \tag{30}$$

证明留给读者。

例 3 求模 $m=2^2\cdot3^2\cdot5^2\cdot7^2$ 的形如式(25)，(30)的既约剩余系。

解 先来构造形如式(25)的既约剩余系。现取 $m_0=2^2$，$m_1=3^2$，$m_2=5^2$，$m_3=7^2$。所以 $M_0=3^2\cdot5^2\cdot7^2$，$M_1=2^2\cdot5^2\cdot7^2$，$M_2=2^2\cdot3^2\cdot7^2$，$M_3=2^2\cdot3^2\cdot5^2$。由第四章 §3 例2 知，可取 $M_0^{-1}=1$，$M_1^{-1}=-2$，$M_2^{-1}=9$，$M_3^{-1}=-19$。容易验证：3^2，5^2，7^2 的原根分别可取2,2,-2。这样，

$$\begin{aligned} x=&\,3^2\cdot5^2\cdot7^2(-1)^{\gamma^{(-1)}}+2^2\cdot5^2\cdot7^2\cdot(-2)\cdot2^{\gamma^{(1)}}+2^2\cdot3^2\cdot7^2\cdot9\cdot2^{\gamma^{(2)}} \\ &+2^2\cdot3^2\cdot5^2\cdot(-19)\cdot(-2)^{\gamma^{(3)}}, \end{aligned} \tag{31}$$

$$0\leqslant\gamma^{(-1)}<2,\quad 0\leqslant\gamma^{(1)}<6,\quad 0\leqslant\gamma^{(2)}<20,\quad 0\leqslant\gamma^{(3)}<42$$

就是所要求的既约剩余系。为了构造形如式(30)的既约剩余系，先要求 $\tilde{g}_j$（注意：由于 $c_0=1$，所以不用求 $\tilde{g}_0$）。为此可利用式(31)。我们有

$$\begin{aligned} \tilde{g}_{-1}\equiv&\,3^2\cdot5^2\cdot7^2\cdot(-1)+2^2\cdot5^2\cdot7^2\cdot(-2)+2^2\cdot3^2\cdot7^2\cdot9 \\ &+2^2\cdot3^2\cdot5^2\cdot(-19) \\ \equiv&-11025-9800+15876-34200 \\ \equiv&-39149\equiv4951 \pmod{44100}, \end{aligned}$$

$$\begin{aligned} \tilde{g}_1\equiv&\,3^2\cdot5^2\cdot7^2+2^2\cdot5^2\cdot7^2\cdot(-2)\cdot2+2^2\cdot3^2\cdot7^2\cdot9 \\ &+2^2\cdot3^2\cdot5^2\cdot(-19) \\ \equiv&\,11025-19600+15876-34200 \\ \equiv&-26899\equiv17201 \pmod{44100}, \end{aligned}$$

$$\begin{aligned} \tilde{g}_2\equiv&\,3^2\cdot5^2\cdot7^2+2^2\cdot5^2\cdot7^2\cdot(-2)+2^2\cdot3^2\cdot7^2\cdot9\cdot2 \\ &+2^2\cdot3^2\cdot5^2\cdot(-19) \\ \equiv&\,11025-9800+31752-34200\equiv-1223 \pmod{44100}, \end{aligned}$$

$$\tilde{g}_3\equiv3^2\cdot5^2\cdot7^2+2^2\cdot5^2\cdot7^2\cdot(-2)+2^2\cdot3^2\cdot7^2\cdot9$$

$$+2^2\cdot3^2\cdot5^2\cdot(-19)(-2)$$
$$\equiv 11025-9800+15876+68400\equiv 85501$$
$$\equiv -2699 \pmod{44100},$$

所以

$$x = 4951^{\gamma^{(-1)}}\cdot 17201^{\gamma^{(1)}}\cdot(-1223)^{\gamma^{(2)}}\cdot(-2699)^{\gamma^{(3)}},$$

$$0\leqslant\gamma^{(-1)}<2,\ 0\leqslant\gamma^{(1)}<6,\ 0\leqslant\gamma^{(2)}<20,\ 0\leqslant\gamma^{(3)}<42$$

就给出了模 $m=2^2\cdot3^2\cdot5^2\cdot7^2=44100$的既约剩余系。

例 4　求模 $m=3\cdot5\cdot7\cdot11=1155$的形如式(25)，式(30)的既约剩余系。

解　先求形如式(25)的既约剩余系。取$m_1=3$，$m_2=5$，$m_3=7$，$m_4=11$。所以，$M_1=5\cdot7\cdot11=385$，$M_2=3\cdot7\cdot11=231$，$M_3=3\cdot5\cdot11=165$，$M_4=3\cdot5\cdot7=105$。由第四章§3例1知，可取$M_1^{-1}=1$，$M_2^{-1}=1$，$M_3^{-1}=2$，$M_4^{-1}=2$。容易验证，3,5,7,11的原根可分别取为$-1,2,-2,2$。这样，

$$\begin{cases} x=5\cdot7\cdot11\cdot(-1)^{\gamma^{(1)}}+3\cdot7\cdot11\cdot2^{\gamma^{(2)}} \\ \quad +3\cdot5\cdot11\cdot2\cdot(-2)^{\gamma^{(3)}}+3\cdot5\cdot7\cdot2\cdot2^{\gamma^{(4)}}, \\ 0\leqslant\gamma^{(1)}<2,\ 0\leqslant\gamma^{(2)}<4,\ 0\leqslant\gamma^{(3)}<6,\ 0\leqslant\gamma^{(4)}<10, \end{cases} \tag{32}$$

就给出了模1155的形如式(25)的既约剩余系。

为了构造形如式(30)的既约剩余系，先要求出满足式(28)与(29)的一组$\bar g_l$ $(1\leqslant l\leqslant4)$，这可利用式(32)。我们有

$$\bar g_1\equiv5\cdot7\cdot11\cdot(-1)+3\cdot7\cdot11+3\cdot5\cdot11\cdot2+3\cdot5\cdot7\cdot2$$
$$\equiv-385+231+330+210\equiv386 \pmod{1155},$$
$$\bar g_2\equiv5\cdot7\cdot11+3\cdot7\cdot11\cdot2+3\cdot5\cdot11\cdot2+3\cdot5\cdot7\cdot2$$
$$\equiv385+462+330+210\equiv1387\equiv232 \pmod{1155},$$
$$\bar g_3\equiv5\cdot7\cdot11+3\cdot7\cdot11+3\cdot5\cdot11\cdot2\cdot(-2)+3\cdot5\cdot7\cdot2$$
$$\equiv385+231-660+210\equiv166 \pmod{1155},$$
$$\bar g_4\equiv5\cdot7\cdot11+3\cdot7\cdot11+3\cdot5\cdot11\cdot2+3\cdot5\cdot7\cdot2\cdot2$$

$\equiv 385+231+330+420\equiv 1366\equiv 211 \pmod{1155}$.

这样，

$$\begin{cases} x=386^{\gamma^{(1)}}\cdot 232^{\gamma^{(2)}}\cdot 166^{\gamma^{(3)}}\cdot 211^{\gamma^{(4)}}, \\ 0\leqslant \gamma^{(1)}<2,\ 0\leqslant \gamma^{(2)}<4,\ 0\leqslant \gamma^{(3)}<6,\ 0\leqslant \gamma^{(4)}<10 \end{cases}$$

就给出了所要的既约剩余系。

在结束本节时，我们来指出：利用本节得到的既约剩余系的表示形式——式(1),(3),(25)及(30)，容易推出第三章§4的Wilson定理及其它结论，即第三章§4的定理1，定理2，定理3，定理4及习题四第11题。这些证明留给读者。但是，这样的证明看来很简洁，但用到了原根的性质，证明这些是并不容易的。所以仍是原来的证明更基本。

习 题 三

1．利用指标的性质及§3例1，构造模23以原根11为底的指标表。

2．列出模13,17,19,41,47,53,71以最小正原根为底的指标表。

3．求模 $m=3\cdot 13\cdot 17$ 的形如§3式(25)和式(30)的既约剩余系。

4．求模 $m=7^2\cdot 11^2$ 的形如§3式(25)和式(30)的既约剩余系。

5．求模 $m=2^6\cdot 43$ 的形如§3式(25)和式(30)的既约剩余系。

6．设模 $m>2$ 存在原根。证明：以任一原根为底，-1 对模m的指标总是$\varphi(m)/2$。

7．列出模2^5,2^7,2^8的指标表。

8．求3对模m的指标组（选定相应的原根）：

(i) $m=2^5\cdot 29\cdot 41^2$；　　(ii) $m=2\cdot 13\cdot 23\cdot 41\cdot 47$。

§4　二项同余方程

设$n\geqslant 2$。我们把同余方程

$$x^n\equiv a(\bmod m) \tag{1}$$

称为模m的二项同余方程。我们已经不止一次地讨论过这种类型的同余方程。例如：第四章§4中的例4($n=2, m=2^l, a=1$)和例5($n=2, m=p^l, p$奇素数，$a=1$)，第四章§5讨论了$n=2$，m是素数p的情形；以及第四章§8的定理7、定理8讨论了m为素数p，$p\nmid a$的情形。利用§3关于指标、指标组的理论可以对二项同余方程(1)作系统的讨论，把这一问题归结为解一次同余方程。

定义1　设$m\geqslant 2$，$(a,m)=1$，$n\geqslant 2$。如果同余方程(1)有解，就称a是模m的n次剩余；如果无解，就称为是模m的n次非剩余。

定理1　设$m\geqslant 2$，$(a,m)=1$，及模m有原根g。那么，同余方程(1)有解，即a是模m的n次剩余的充要条件是

$$(n,\phi(m))\mid\gamma(a), \tag{2}$$

这里$\gamma(a)=\gamma_{m,g}(a)$是$a$对模$m$的以$g$为底的指标。此外，有解时(1)恰有$(n,\phi(m))$个解。

证　若$x\equiv x_1(\bmod m)$是(1)的解，由$(a,m)=1$知$(x_1,m)=1$，所以，由§3定理5知，必有y_1使得

$$x_1\equiv g^{y_1}(\bmod m). \tag{3}$$

因而有

$$g^{ny_1}\equiv a(\bmod m), \tag{4}$$

进而由§3性质1知

$$ny_1\equiv\gamma(a)(\bmod \phi(m)).$$

这表明$y\equiv y_1(\bmod \phi(m))$是一次同余方程

$$ny\equiv\gamma(a)(\bmod \phi(m)) \tag{5}$$

的解。反过来，若$y\equiv y_1(\bmod \phi(m))$是(5)的解，则同样由§3性

质1推出有式(4)成立。因此，当x_1由式(3)给出时，$x\equiv x_1 \pmod m$必是(1)的解。这就证明了同余方程(1)($(a,m)=1$)与同余方程(5)同时有解或无解。此外，对任意的

$$x_2\equiv g^{y_2}\pmod m,$$

由§1性质4(取$a=g$)知，$x_1\equiv x_2\pmod m$的充要条件是$y_1\equiv y_2\pmod{\phi(m)}$。因此，同余方程(1)($(a,m)=1$)有解时和同余方程(5)的解数相同。

由第四章§2定理2知，(5)有解的充要条件是式(2)成立，且有解时恰有$(n,\phi(m))$个解。由此及前面的讨论就证明了定理。

定理1给出了当模m有原根时具体求解方程(1)($(a,m)=1$)的方法：(i)利用指标表找出a的指标$\gamma(a)$；(ii)解同余方程(5)；(iii)若(5)有解，则对每个解$y_1\pmod{\phi(m)}$利用指标表找出x_1满足式(3)。这样得到的所有的$x_1\pmod m$就是(1)的全部解。

例1 解同余方程$x^8\equiv 41\pmod{23}$。

解 由§2例1知，5是模23的原根，$41\equiv -5\pmod{23}$，从§3例1的表2中找出$\gamma_{23,5}(41)=12$。所以，要解同余方程

$$8y\equiv 12\pmod{22}.$$

由于$(8,22)=2|12$，所以上述同余方程有解，解数为2。容易看出，它的两个解是

$$y\equiv -4,7\pmod{22}.$$

从§3例1的表1中找出指标为18($18\equiv -4\pmod{22}$)的数是6；指标为7的数是-6。所以原方程的全部解为

$$x\equiv -6,6\pmod{23}.$$

在模m有原根g时，

$$a=g^j,\quad 0\leqslant j<\phi(m) \tag{6}$$

是它的一个既约剩余系，$\gamma(a)=j$。因此，由定理1知，a是模m的n次剩余的充要条件是$(n,\phi(m))|j$。所以在式(6)给出的$\phi(m)$个数中恰有以下$\phi(m)/(n,\phi(m))$个数是模m的n次剩余：

$$a=g^j,\quad j=t\cdot(n,\phi(m)),$$
$$0\leqslant t<\phi(m)/(n,\phi(m)).$$

这样，我们就证明了

定理2 设模 m 有原根，$n\geqslant 2$。那么，在模 m 的一个既约剩余系中，模 m 的 n 次剩余恰有 $\phi(m)/(n,\phi(m))$ 个。

例如，模23的八次剩余有11个，它们是

$$a\equiv 5^{2t}\pmod{23},\quad 0\leqslant t<11,$$

由§3例1的表1可查出

$$a\equiv 1,2,4,8,-7,9,-5,-10,3,6,-11\pmod{23}. \tag{7}$$

当模 m 有原根时，指数与指标之间有关系（§3性质4）：

$$\phi(m)=(\phi(m),\gamma(a))\cdot\delta_m(a).$$

因此，$(n,\phi(m))\mid\gamma(a)$成立的充要条件是存在整数 s 使得

$$\frac{\phi(m)}{(n,\phi(m))}=s\cdot\delta_m(a),$$

即

$$\delta_m(a)\,\Big|\,\frac{\phi(m)}{(n,\phi(m))}. \tag{8}$$

进而，由§1性质2知，式(8)成立的充要条件是

$$a^{\phi(m)/(n,\phi(m))}\equiv 1\pmod m. \tag{9}$$

这样，就证明了

定理3 设模 m 有原根，$n\geqslant 2$。那么，a是模 m 的 n 次剩余，即二项同余方程($(a,m)=1$)有解的充要条件是式(9)(即式(8))成立，且有解时有$(n,\phi(m))$个解。

当$m=23$，$n=8$时，$\phi(23)/(8,\phi(23))=11$。由§3例1的表1知，满足$\delta_{23}(a)\mid 11$的全体 a 正好是由式(7)给出。

当 m 为素数 p 时，定理2和3已在第四章§8定理7、8及9中证明，这里利用原根再一次证明了这些结论。

下面来讨论 $m=2^{\alpha}$ $(\alpha\geqslant 3)$ 的情形。

定理4 设$m=2^\alpha$，$\alpha\geqslant 3$，$2\nmid a$，以及a对模2^α的以$-1,5$为底的指标组是$\gamma^{(-1)}(a)$，$\gamma^{(0)}(a)$。那么，a是模2^α的n次剩余，即二项同余方程(1)有解的充要条件是

$$(n,2)\mid\gamma^{(-1)}(a),\quad (n,2^{\alpha-2})\mid\gamma^{(0)}(a),\tag{10}$$

且有解时恰有$(n,2)\cdot(n,2^{\alpha-2})$个解。也就是说，当$2\nmid n$时，总有解且恰有一解；当$2\mid n$时，若有解则有$2\cdot(n,2^{\alpha-2})$个解。

证[①] 由$2\nmid a$知，只要x在模2^α的一个既约剩余系中取值时，讨论方程(1)。所以可设(为什么)

$$x=(-1)^u5^v,\quad 0\leqslant u<2,\quad 0\leqslant v<2^{\alpha-2}.\tag{11}$$

这样，方程(1)就变为一个有两个变数的同余方程：

$$\begin{cases}(-1)^{nu}5^{nv}\equiv(-1)^{\gamma^{(-1)}(a)}5^{\gamma^{(0)}(a)}\pmod{2^\alpha},\\ 0\leqslant u<2,\quad 0\leqslant v<2^{\alpha-2}.\end{cases}\tag{12}$$

由§3性质5知，方程(12)。就是同余方程组

$$\begin{cases}nu\equiv\gamma^{(-1)}(a)\pmod 2,\quad 0\leqslant u<2,\\ nv\equiv\gamma^{(0)}(a)\pmod{2^{\alpha-2}},\quad 0\leqslant v<2^{\alpha-2}.\end{cases}\tag{13}$$

由第四章§2定理2知，第一个一次同余方程（注意u正好在模2的一个完全剩余系中取值）有解的充要条件是

$$(n,2)\mid\gamma^{(-1)}(a),\tag{14}$$

有解时有$(n,2)$个解；第二个一次同余方程（注意v正好在模$2^{\alpha-2}$的一个完全剩余系中取值）有解的充要条件是

$$(n,2^{\alpha-2})\mid\gamma^{(0)}(a),\tag{15}$$

有解时有$(n,2^{\alpha-2})$个解。所以，同余方程组(13)，即同余方程(12)，也即同余方程(1)有解的充要条件是式(14),(15)同时成立，即式(10)成立。有解时解数应为方程组(13)中两个方程的解数的乘积，即$(n,2)\cdot(n,2^{\alpha-2})$，证毕。

例2 解同余方程$x^{12}\equiv 17\pmod{2^6}$。

---

① 这一证法与定理1的证法是一样的，只是表述的不同。

解　由§3例2的表4查得17的指标组是$\gamma^{(-1)}(17)=0,\gamma^{(0)}(17)=12$。因此，要解两个一次同余方程：

$$12u\equiv 0(\mathrm{mod}\ 2),\quad 0\leqslant u<1.$$
$$12v\equiv 12(\mathrm{mod}\ 2^4),\quad 0\leqslant v<2^4.$$

易知，$u=0,1$；$v=1,5,9,13$。这样，由式(11)就给出x的八个解，查§3例2的表3得到这八个解是

$$x\equiv 5,-11,-27,21,-5,11,27,-21(\mathrm{mod}\ 2^6).$$

例3　解同余方程$x^{11}\equiv 27(\mathrm{mod}\ 2^6)$。

解　查§3例2的表4得$\gamma^{(-1)}(27)=1$，$\gamma^{(0)}(27)=9$。因此，要解两个一次同余方程

$$11u\equiv 1(\mathrm{mod}\ 2),\quad 0\leqslant u<1.$$
$$11v\equiv 9(\mathrm{mod}\ 2^4),\quad 0\leqslant v<2^4.$$

容易解得$u=1$，$v=11$。这样，由式(11)给出的x就是原方程的解。查§3例2的表3得到解$x\equiv -29(\mathrm{mod}\ 2^6)$。

定理5　设$m=2^\alpha,\alpha\geqslant 3$。那么，当$2\nmid n$时模$2^\alpha$的一个既约剩余系中的全部元素都是模$2^\alpha$的$n$次剩余；当$2|n$时，模$2^\alpha$的一个既约剩余系中有$2^{\alpha-2}/(n,2^{\alpha-2})$个元素是模$2^\alpha$的$n$次剩余。

证　当$2\nmid n$时，条件(10)总成立，所以结论成立。当$2|n$时，条件(10)要成立当且仅当$\gamma^{(-1)}(a)=0$及$(n,2^{\alpha-2})|\gamma^{(0)}(a)$，$0\leqslant\gamma^{(0)}(a)<2^{\alpha-2}$，所以恰有$2^{\alpha-2}/(n,2^{\alpha-2})$组这样的指标组，即在模$2^\alpha$的一个既约剩余系中恰有$2^{\alpha-2}/(n,2^{\alpha-2})$个元素是模$2^\alpha$的$n$次剩余。证毕。

例如，模2^6的12次剩余a的指标组应满足

$$(12,2)=2|\gamma^{(-1)}(a),\quad (12,2^4)=4|\gamma^{(0)}(a).$$

因此，有$\gamma^{(-1)}(a)=0$；$\gamma^{(0)}(a)=0,4,8,12$。查§3例2的表3得模2^6的12次剩余有四个，它们是：

$$a\equiv 1,-15,-31,17(\mathrm{mod}\ 2^6).\qquad (16)$$

定理6　设$m=2^\alpha,\alpha\geqslant 3,2|n$，及$2^\lambda=(n,2^{\alpha-2})$。那么，$a$是

模2^α的n次剩余，即二项同余方程(1)有解的充要条件是

$$a\equiv 1(\bmod 2^{\lambda+2}). \tag{17}$$

证 *必要性* 由定理4知，这时 $\gamma^{(-1)}(a)=0$，及

$$a\equiv 5^{t\cdot 2^\lambda}(\bmod 2^\alpha).$$

由于 $\lambda\leqslant\alpha-2$，及

$$5^{2^\lambda}\equiv 1(\bmod 2^{\lambda+2}),$$

从上式就推出式(17)成立。

充分性 若式(17)成立，由于$\lambda\geqslant 1$(因为$2|n,\alpha\geqslant 3$)，所以，$\gamma^{(-1)}(a)=0$，因而有

$$a\equiv 5^{\gamma^{(0)}(a)}(\bmod 2^\alpha).$$

由于 $\lambda+2\leqslant\alpha$，所以从上式及式(17)推出

$$5^{\gamma^{(0)}(a)}\equiv 1(\bmod 2^{\lambda+2}).$$

由§1例6知$\delta_{2^{\lambda+2}}(5)=2^\lambda$（这里 $\lambda\geqslant 1$），由此及上式，从§1性质3推得 $2^\lambda|\gamma^{(0)}(a)$。这样，由定理4推出$a$是模$2^\alpha$的$n$次剩余。这就证明了充分性。证毕。

由定理6知，模2^6的12次剩余a应是

$$a\equiv 1(\bmod 2^4),$$

因为$2^\lambda=(12,2^4)=2^2,\lambda=2$。这和式(16)得到的结果相同。

利用指数与指标组之间的关系(§3性质5、7)，像证明定理3一样，从定理4可以推出：

定理7 设$m=2^\alpha,\alpha\geqslant 3,2\nmid a$。那么，$a$是模$2^\alpha$的$n$次剩余，即二项同余方程(1)有解的充要条件是：

$$(a-1)/2\equiv 0(\bmod (n,2)),\quad \delta_{2^\alpha}(a)|2^{\alpha-2}/(n,2^{\alpha-2}). \tag{18}$$

也就是条件：

$$(a-1)/2\equiv 0(\bmod (n,2)),\quad a^{2^{\alpha-2}/(n,2^{\alpha-2})}\equiv 1(\bmod 2^\alpha). \tag{19}$$

证 由§3性质7知：

$$2^{\alpha-2}=(2^{\alpha-2},\gamma^{(0)}(a))\delta_{2^\alpha}(a),\quad \gamma^{(0)}(a)\neq 0. \tag{20}$$

$$2=(2,\gamma^{(-1)}(a))\delta_{2^\alpha}(a),\quad \gamma^{(0)}(a)=0. \tag{21}$$

我们来证明条件(18)的充要性。条件(18)与(19)的等价性证明留

给读者。先证必要性。由定理 4 知(10)成立。由式(10)的第一式及 § 3式(13)推出式(18)的第一式成立。当$\gamma^{(0)}(a)\neq0$时由式(10)的第二式及式(20)推出式(18)的第二式成立。当$\gamma^{(0)}(a)=0$时，$a\equiv\pm1(\bmod 2^{\alpha})$。若 n 为奇，则式(18)的第二式总成立；若 n 为偶，则由式(18)的第一式推出 $a\equiv1(\bmod 2^{2})$，所以$a\equiv1(\bmod 2^{\alpha})$。因此，$\delta_{2^{\alpha}}(a)=1$，所以式 (18) 的第二式也成立。这就证明了必要性。下证充分性。设式(18)成立。由式(18)第一式及 § 3式(13)推出式(10)第一式成立。若$\gamma^{(0)}(a)=0$时，式(10)的第二式总成立；若$\gamma^{(0)}(a)\neq0$，则由式(18)的第二式及式(20)推出式(10)的第二式成立。所以式(10)总成立。由此及定理 4 就证明了充分性。

显见，当 n 为奇数时，条件(18)，(19)都一定成立。我们也可以利用定理 6 来证明定理 7，详细推导留给读者。

习　题　四

1．利用指标表解以下同余方程：

(i) $3x^6\equiv5(\bmod 7)$；　(ii) $x^{12}\equiv16(\bmod 17)$；

(iii) $5x^{11}\equiv-6(\bmod 17)$；　(iv) $3x^{14}\equiv2(\bmod 23)$；

(v) $x^{15}\equiv14(\bmod 41)$；　(vi) $7x^7\equiv11(\bmod 41)$；

(vii) $3^x\equiv2(\bmod 23)$；　(viii) $13^x\equiv5(\bmod 23)$。

2．对哪些整数 a，同余方程 $ax^5\equiv3(\bmod 19)$可解？

3．对哪些整数 b，同余方程 $7x^8\equiv b(\bmod 41)$可解？

4．求同余方程 $x^x\equiv x(\bmod 19)$满足$(x,19)=1$的全部解。

5．求同余方程 $5^x\equiv x(\bmod 23)$的全部解。

6．设素数 $p>2$。证明：同余方程 $x^4\equiv-1(\bmod p)$ 有解的充要条件是 $p\equiv1(\bmod 8)$。由此推出形如 $p\equiv1(\bmod 8)$ 的素数有无穷多个。

7．解同余方程：

(i) $x^6\equiv-15(\bmod 64)$；　(ii) $x^{12}\equiv7(\bmod 128)$。

8．解同余方程：

(i) $3x^6\equiv 7 \pmod{2^5\cdot 31}$；　　(ii) $5x^4\equiv 3 \pmod{2^5\cdot 23\cdot 19}$.

9．利用原根求出以下模 m 的全部三次、四次剩余：

$$m=13,17,19,23,41,43,17^2,23^2,41^2,43^2.$$

10．求模 53^2 的26次剩余．

11．若素数 $p\equiv 5 \pmod 8$，则同余方程 $x^4\equiv -1 \pmod p$ 无解．

12．设 p 是素数，证明：同余方程 $x^8\equiv 16 \pmod p$ 一定有解．

13．设 p 是素数，$2\nmid \delta_p(a)$．证明：同余方程 $a^x+1\equiv 0 \pmod p$ 无解．

14．求同余方程 $5^x\equiv 3^x+2 \pmod{11}$ 的全部解．

15．对哪些整数 a，同余方程 $10^x\equiv a \pmod{41}$ 有解？

16．证明：2是模73的8次剩余．

17．用利用原根和不利用原根两种方法来解同余方程：

(i) $x^4\equiv 41 \pmod{37}$；　　(ii) $x^4\equiv 37 \pmod{41}$．

18．解同余方程 $(x^2+1)(x+1)x\equiv -1 \pmod{41}$．

19．设素数 $p\equiv 3 \pmod 4$．证明：a 是模 p 的四次剩余的充要条件是 $\left(\frac{a}{p}\right)=1$，即 a 是模 p 的二次剩余．求解同余方程

$$x^4\equiv 3 \pmod{11}.$$

第六章 不定方程（Ⅱ）

本章应用同余理论讨论四个基本的、重要的不定方程：§1中的$x_1^2+x_2^2+x_3^2+x_4^2=n$；§2和§3中的$x^2+y^2=n$，并求出了它的解数公式；§4中的$ax^2+by^2+cz^2=0$；以及§5中的$x^3+y^3=z^3$。从本章的讨论可以看出，如果不用同余理论，而直接利用整除性质（像第二章所做的那样）去研究这些不定方程，那么不是不可能的话，也是极为复杂困难的。

§1 $x_1^2+x_2^2+x_3^2+x_4^2=n$

本节要证明以下结论：

定理1 每个正整数一定可表为四个平方数之和，即对任意的$n\geqslant 1$，不定方程

$$x_1^2+x_2^2+x_3^2+x_4^2=n \tag{1}$$

有解。

容易直接验证下面的恒等式成立：

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)\\ =(a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2\\ +(a_1b_3-a_3b_1+a_4b_2-a_2b_4)^2+(a_1b_4-a_4b_1+a_2b_3-a_3b_2)^2.\end{aligned} \tag{2}$$

由此推出：若两个整数都可表为四个平方数之和，那么它们的乘积也一定是四个平方数之和。由于$1=1^2+0^2+0^2+0^2$，所以定理1等价于下面的

定理2 每个素数p一定可表为四个平方数之和，即当$n=p$时不定方程(1)有解。

由于$2=1^2+1^2+0^2+0^2$，所以为证定理2可以假定$p>2$。先

来证明两个引理。

引理3 设素数 $p>2$。同余方程

$$\begin{cases}x^2+y^2+1\equiv 0\pmod p,\\ 0\leqslant x,y\leqslant (p-1)/2\end{cases}$$

有解。

证 容易看出，以下 $(p+1)/2$ 个数对模 p 两两不同余：

$$a^2,\qquad a=0,1,\cdots,(p-1)/2.$$

同样，以下 $(p+1)/2$ 个数也对模 p 两两不同余：

$$-b^2-1,\qquad b=0,1,\cdots,(p-1)/2.$$

但在这总共 $p+1$ 个数中必有两个数对模 p 同余，因此，一定有一个 $a_0^2\ (0\leqslant a_0\leqslant (p-1)/2)$ 和一个 $-b_0^2-1\ (0\leqslant b_0\leqslant (p-1)/2)$ 对模 p 同余。取 $x=a_0, y=b_0$ 就证明了引理。

引理4 设素数 $p>2$。一定存在整数 x_0, y_0 及 m_0，$1\leqslant m_0<p$，使得

$$m_0p=1+x_0^2+y_0^2.$$

证 取 x_0, y_0 是引理3中的同余方程的解。我们有

$$x_0^2+y_0^2+1=m_0p,\qquad m_0\geqslant 1.$$

但另一方面

$$x_0^2+y_0^2+1\leqslant\left(\frac{p-1}{2}\right)^2+\left(\frac{p-1}{2}\right)^2+1$$

$$=p^2/2-p+3/2<p^2/2.$$

由以上两式得 $1\leqslant m_0<p/2$。证毕。

定理2的证明 设 $p>2$。由引理4知必有正整数 $m_0<p$，及整数 x_1,x_2,x_3,x_4 使得

$$m_0p=x_1^2+x_2^2+x_3^2+x_4^2.\tag{3}$$

设 m_0 是所有使式(3)成立的这种数中的最小的。我们来证明必有 $m_0=1$。分以下几步来证。

(i) 必有 $(x_1,x_2,x_3,x_4)=1$。若不然，有素数 $q\mid(x_1,x_2,x_3,x_4)$。

由此及式(3)知 $q^2 | m_0 p$。一定有 $q \neq p$。若不然，由 $q = p$ 推出 $p | m_0$，这和 $1 < m_0 < p$ 矛盾。因而有 $q^2 | m_0$，所以得

$$\left(\frac{m_0}{q^2}\right)p = \left(\frac{x_1}{q}\right)^2 + \left(\frac{x_2}{q}\right)^2 + \left(\frac{x_3}{q}\right)^2 + \left(\frac{x_4}{q}\right)^2.$$

但这和 m_0 的最小性矛盾。

(ii) m_0 一定是奇数。若 m_0 是偶数，则 x_1, x_2, x_3, x_4 中的奇数的个数必为偶数个(包括没有奇数的情形)。所以可假定 $2 | x_1 + x_2$，$2 | x_3 + x_4$。由此及式(3)就推出

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

这又和 m_0 的最小性矛盾。

(iii) 必有 $m_0 = 1$。若不然，设 $m_0 > 1$，由(i)知 $m_0 \nmid (x_1, x_2, x_3, x_4)$。现取(注意 m_0 是奇数)

$$y_j \equiv x_j \pmod{m_0}, \quad |y_j| < m_0/2, \quad j = 1,2,3,4. \tag{4}$$

我们有 $y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2$ 及

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

所以有

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0, \quad 0 \leqslant m_1 < m_0. \tag{5}$$

我们来证明 $m_1 \neq 0$。若 $m_1 = 0$，则 $y_1 = y_2 = y_3 = y_4 = 0$。由此及式(4)得 $m_0 | x_j$，$j = 1,2,3,4$。但这和 $m_0 \nmid (x_1, x_2, x_3, x_4)$ 矛盾(因为假设 $m_0 > 1$)。

在式(2)中取 $a_j = x_j$，$b_j = y_j$，$j = 1,2,3,4$，由式(3)及(5)得

$$u_1^2 + u_2^2 + u_3^2 + u_4^2 = m_1 m_0^2 p, \quad 1 \leqslant m_1 < m_0, \tag{6}$$

其中

$$u_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \quad u_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3,$$
$$u_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4, \quad u_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2.$$

由式(4)及式(3)得

$$u_1 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

由式(4)得 $x_i y_j \equiv x_j y_i \pmod{m_0}$，$1 \leqslant i, j \leqslant 4$，因而有

$$u_2 \equiv u_3 \equiv u_4 \equiv 0 \pmod{m_0}.$$

由以上两式及式(6)得到

$$(u_1/m_0)^2 + (u_2/m_0)^2 + (u_3/m_0)^2 + (u_4/m_0)^2 = m_1 p_1, \quad 1 \leqslant m_1 < m_0.$$

这和 m_0 的最小性矛盾。所以 $m_0 = 1$。定理证毕。

定理1和定理2中的"四"是不能改进的，这可由下面的结论看出。

定理5 当 n 是形如 $4^a(8k+7)(a \geqslant 0, k \geqslant 0)$ 的正整数时，n 不能表为三个整数的平方和。

证 对任意整数 x 有

$$x^2 \equiv 0, 1 \text{ 或 } 4 \pmod 8. \tag{7}$$

因此，对任意整数 x_1, x_2, x_3 必有

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8.$$

由此推出，n 是形如 $8k+7$ 的正整数时不能表为三个整数的平方和，即定理当 $a=0$ 时成立。假设定理当 $a=l(l \geqslant 0)$ 时成立。当 $a=l+1$ 时，若有 $n=4^{l+1}(8k_1+7)$ 可表为

$$n = 4^{l+1}(8k_1+7) = x_1^2 + x_2^2 + x_3^2,$$

则由式(7)及 $x_1^2 + x_2^2 + x_3^2 \equiv 0$ 或 $4 \pmod 8$ 推出

$$x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod 2.$$

因而有

$$4^l(8k_1+7) = (x_1/2)^2 + (x_2/2)^2 + (x_3/2)^2.$$

但这和归纳假设矛盾，所以定理对 $a=l+1$ 也成立。证毕。

由定理5立即推出定理1中的"四"是最佳结果。由于 $8k+7$ 形式的素数有无穷多个(为什么)，所以定理2中的"四"也是不能改进的。

在定理1和2都没有要求 n（或 p）表为四个正整数的平方之和，即没有要求式(1)中的 $x_i(1 \leqslant i \leqslant 4)$ 都是正整数。事实上，这

是不可能的，利用归纳法容易证明(留给读者)：

定理6 $n=2\cdot 4^a(a\geq 0)$不能表为四个正平方数之和。

但我们可以证明下面的结论：

定理7 除去以下十二个数：

$$1,2,3,4,6,7,9,10,12,15,18,33 \tag{8}$$

之外，每个正整数都是五个正平方数之和。

定理可以这样证明：由式(8)给出的十二个数可直接验证，它们都不能表为五个正平方数之和；当$n\leq 168$且不等于上述十二个数时，直接验证它们都能表为五个正平方数之和；利用

$$\begin{aligned}169 = 13^2 &= 12^2+5^2 = 12^2+4^2+3^2\\ &= 11^2+4^2+4^2+4^2\\ &= 10^2+6^2+4^2+4^2+1^2,\end{aligned}$$

及定理1，就可推出结论当$n\geq 169$时一定成立。具体论证留给读者。

由定理6知，定理7中的“五”是不能改进的。

习　题　一

1．设素数$p>2$，a是整数。证明下面的同余方程有解：

$x^2+y^2+a\equiv 0\pmod p$，　$0\leq x,y\leq (p-1)/2$。

2．写出§1定理6的证明。

3．(i) 验证由§1式(8)给出的十二个数一定不是五个正平方数之和。

(ii) 验证除去(i)中的十二个数以外，正整数$n\leq 168$一定是五个正平方数之和。

4．把(i) $23\cdot 53$，(ii) $43\cdot 197$，(iii) $47\cdot 223$分别表为两种不同形式的四个平方数之和。

5．设$2\nmid t$，$(x,y,z)=1$。证明：$t^2=x^2+y^2+z^2$不可能成立。

6．证明：除去有限个例外值之外，每个正整数都是六个正

平方数之和。求出这些例外值。

7．证明：$2^k(k\geqslant 0)$一定不能表为三个正平方数之和，并直接求出$2^k=x_1^2+x_2^2+x_3^2+x_4^2$的全部解。

8．证明：存在无穷多个n使得$n=x_1^2+x_2^2+x_3^2+x_4^2$没有满足条件(i) $(x_1,x_2,x_3,x_4)=1$的解，也没有满足条件(ii) $x_1>x_2>x_3>x_4\geqslant 0$的解。

§2　$x^2+y^2=n$ (A)

我们先来证明以下结论：

定理1　设p是素数，那么，不定方程

$$x^2+y^2=p \tag{1}$$

有解的充要条件是$p=2$或$\left(\frac{-1}{p}\right)=1$，即$p=2$或$p=4k+1$。

证　必要性　由于p是素数，所以不定方程(1)若有解x_0，y_0，则必满足

$$(x_0,y_0)=(x_0y_0,p)=1. \tag{2}$$

因而必有y_0^{-1}满足$y_0^{-1}y_0\equiv 1 \pmod p$，由此得

$$(x_0y_0^{-1})^2+1+kp=(y_0^{-1})^2p.$$

若$p>2$，由上式得

$$(x_0y_0^{-1})^2\equiv -1 \pmod p,$$

即$\left(\frac{-1}{p}\right)=1$，亦即$p=4k+1$(见第四章§5推论3)，这就证明了必要性。

充分性　当$p=2$时有$2=1^2+1^2$，所以(1)有解。当$p>2$时，由$\left(\frac{-1}{p}\right)=1$(即$p=4k+1$)知，必有$x$满足

$$x^2+1\equiv 0 \pmod p,\quad 0<|x|<p/2.$$

由此推出，必有$p>m_0\geqslant 1$及x,y满足

$$x^2+y^2=m_0p. \tag{3}$$

设 m_0 是使上式成立的最小正整数。如果能证明 $m_0=1$，则就证明了充分性。这时，和§1定理2的证明中的(i)一样可证 $(x,y)=1$（留给读者）。下面用反证法来证 $m_0=1$。若 $m_0>1$，取

$$\begin{cases} u\equiv x \pmod{m_0}, & |u|\leqslant m_0/2, \\ v\equiv y \pmod{m_0}, & |v|\leqslant m_0/2. \end{cases} \tag{4}$$

由此及 $(x,y)=1$ 立即推出

$$0<u^2+v^2\leqslant m_0^2/2,$$
$$u^2+v^2\equiv x^2+y^2 \pmod{m_0}.$$

进而利用式(3)得

$$(u^2+v^2)(x^2+y^2)=m_1m_0^2p, \qquad 1\leqslant m_1<m_0.$$

利用熟知的恒等式

$$(a_1^2+a_2^2)(b_1^2+b_2^2)=(a_1b_1+a_2b_2)^2+(a_1b_2-a_2b_1)^2, \tag{5}$$

上式变为

$$(ux+vy)^2+(uy-vx)^2=m_1m_0^2p.$$

由式(4)及式(3)知

$$ux+vy\equiv x^2+y^2\equiv 0 \pmod{m_0},$$
$$uy-vx\equiv 0 \pmod{m_0}.$$

因而有

$$\left(\frac{ux+vy}{m_0}\right)^2+\left(\frac{uy-vx}{m_0}\right)^2=m_1p, \qquad 1\leqslant m_1<m_0.$$

而这和 m_0 的最小性矛盾。所以 $m_0=1$。证毕。

怎样的正整数 n 才能表为两个平方数之和呢？即对怎样的 n，不定方程

$$x^2+y^2=n, \qquad x,y\in \boldsymbol{Z} \tag{6}$$

才有解？由定理1及式(5)可得以下结论：

定理2 设正整数 $n=d^2m$，m 无平方因数。那么，不定方程(6)有解的充要条件是 m 没有形如 $4k+3$ 的素因数。

证 充分性 由条件知

$$m=2^{a}p_1\cdots p_r,\qquad p_j\equiv 1\pmod 4,$$
$$1\leqslant j\leqslant r,\qquad 0\leqslant a\leqslant 1.$$
式(5)表明：若 $n=n_1,n=n_2$ 时不定方程(6)均可解，则当$n=n_1n_2$ 时不定方程(6)也可解。由定理 1 知，当 $n=2,p_1,\cdots,p_r$ 时不定方程(6)均有解，因此，反复利用式(5)就推出当 $n=m$ 时不定方程(6)有解。设
$$m=x_1^2+y_1^2,$$
因而有
$$n=d^2m=(dx_1)^2+(dy_1)^2.$$
这就证明了充分性。

必要性　设 $n=d^2m$ 时不定方程(6)有解
$$x_1^2+y_1^2=d^2m.$$
设 $c=(x_1,y_1)$，$x_1=c\bar{x}_1$，$y_1=c\bar{y}_1$。由于 m 无平方因数，所以必有 $c\mid d$。设 $d=c\bar{d}$，我们有
$$\bar{x}_1^2+\bar{y}_1^2=\bar{d}^2m,\qquad (\bar{x}_1,\bar{y}_1)=1.$$
若 m 有素因数 $p\equiv 3\pmod 4$，则由上式得 $p\nmid \bar{x}_1\bar{y}_1$ 及
$$\bar{x}_1^2\equiv-\bar{y}_1^2\pmod p.$$
由第四章§6定理 1 的(i),(iii),(iv)及(v)得
$$1=\left(\frac{\bar{x}_1^2}{p}\right)=\left(\frac{-\bar{y}_1^2}{p}\right)=\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}.$$
由上式得 $p\equiv 1\pmod 4$，矛盾。这就证明了必要性。

一个很自然的问题是不定方程(6)何时才有满足条件 $(x,y)=1$ 的解呢？

定理3　不定方程(6)有满足条件 $(x,y)=1$ 的解的充要条件是 $n=1,2,n_1$ 或 $2n_1$，其中
$$n_1=p_1^{a_1}\cdots p_r^{a_r},\qquad p_j\equiv 1\pmod 4,\ 1\leqslant j\leqslant r.$$

证　必要性　这就是要证明 $4\nmid n$ 及 n 没有形如 $4k+3$ 的素

因数。这时必有$(x,y)=(x,n)=(y,n)=1$。若$4|n$，则有

$$x^2-y^2\equiv 0\pmod 4,$$

但这当$(x,2)=(y,2)=1$时是不可能的，所以必有$4\nmid n$，若有$p\equiv 3\pmod 4$，$p|n$，我们就有$(p,x)=(p,y)=1$，及

$$x^2+y^2\equiv 0\pmod p.$$

同定理2的必要性证明完全一样，可推出必有$p\equiv 1\pmod 4$，矛盾。

充分性 $1=1^2+0^2$，$2=1^2+1^2$，结论当然成立。先用归纳法来证明：当$n=p^\alpha$，$p\equiv 1\pmod 4$时，

$$x^2+y^2=p^\alpha,\qquad (x,y)=1 \tag{7}$$

有解。$\alpha=1$时，这就是定理1，所以有解。设结论对$\alpha=k$时成立。我们来证结论对$\alpha=k+1$也成立。设

$$x_1^2+y_1^2=p,\qquad (x_1,y_1)=1, \tag{8}$$

$$x_k^2+y_k^2=p^k,\qquad (x_k,y_k)=1. \tag{9}$$

由此及式(5)知

$$(x_1x_k+y_1y_k)^2+(x_1y_k-y_1x_k)^2=p^{k+1}, \tag{10}$$

$$(x_1x_k-y_1y_k)^2+(x_1y_k+y_1x_k)^2=p^{k+1}. \tag{11}$$

这时，

$$d_1=(x_1x_k+y_1y_k,\ x_1y_k-y_1x_k)=1$$

或

$$d_2=(x_1x_k-y_1y_k,\ x_1y_k+y_1x_k)=1$$

至少有一个成立。若不然，$d_1>1$，$d_2>1$，则由式(10)及(11)知$p|d_1$，$p|d_2$。因而有$p|2x_1x_k$，所以$p|x_1$或$p|x_k$至少有一个成立，但由式(8)及(9)知是不可能的。因此，当$d_1=1$时，由式(10)知结论对$\alpha=k+1$成立，当$d_2=1$时，由式(11)知结论对$\alpha=k+1$成立。这就证明了对任意的$\alpha\geqslant 1$不定方程(7)总有解。

再来证明：若$(n_1,n_2)=1$，及

$$x_1^2+y_1^2=n_1,\qquad (x_1,y_1)=1, \tag{12}$$

$$x_2^2+y_2^2=n_2,\qquad (x_2,y_2)=1, \tag{13}$$

那么，当 $n=n_1n_2$ 时不定方程(6)必有满足 $(x,y)=1$ 的解。由式(5)知

$$(x_1x_2+y_1y_2)^2+(x_1y_2-y_1x_2)^2=n_1n_2. \tag{14}$$

若 $d=(x_1x_2+y_1y_2,\ x_1y_2-y_1x_2)>1$，则必有素数 $q|d$。因此有

$$x_1x_2\equiv -y_1y_2 \pmod q, \tag{15}$$

$$x_1y_2\equiv y_1x_2 \pmod q. \tag{16}$$

这时必有 $q\nmid x_1$，若不然，设 $q|x_1$，由以上两式得 $q|y_1y_2, q|y_1x_2$，由此及 $(x_1,y_1)=1$ 推出 $q|y_2$，$q|x_2$，这和 $(x_2,y_2)=1$ 矛盾。同理可证 q 不能整除 y_1, x_2 及 y_2。由式(15)及(16)易得

$$x_1(x_2^2+y_2^2)\equiv 0 \pmod q,$$

$$x_2(x_1^2+y_1^2)\equiv 0 \pmod q.$$

由此及 $q\nmid x_1x_2$ 得（注意：q 是素数）

$$x_1^2+y_1^2\equiv x_2^2+y_2^2\equiv 0 \pmod q.$$

由此及式(12)，(13)得 $n_1\equiv n_2\equiv 0 \pmod q$，这和 $(n_1,n_2)=1$ 矛盾，所以 $d=1$。由此及式(14)就证明了所要结论。

综合以上的讨论就证明了充分性。证毕。

以上我们讨论了如何判别一个正整数能否表为两个平方数之和，以及在能表出时，如何具体来求出这种表示。问题的关键在于如何把形如 $4k+1$ 的素数 p 表为两个平方数之和，当 p 不大时可以直接试算，而一般地给出一个公式是比较困难的。这将在习题中给出。

一个更进一步的问题是：不定方程(6)的解数是多少？我们将在下一节利用同余方程理论来解决这一问题。

作为本节的结束，类似于定理 1 我们可以证明下面的定理：

定理4 设素数 $p>3$。那么，不定方程

$$x^2+3y^2=p \tag{17}$$

有解的充要条件是$\left(\frac{-3}{p}\right)=1$，即 p 是形如 $6k+1$ 的素数。

证　*必要性*　若不定方程(17)有解 x_0, y_0，则显然有

$$(x_0, 3y_0)=(p, 3x_0y_0)=1.$$

利用第四章§6定理1，由此及式(17)得

$$1=\left(\frac{x_0^2}{p}\right)=\left(\frac{-3y_0^2}{p}\right)=\left(\frac{-3}{p}\right).$$

再利用第四章§6定理1和定理5可得

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\cdot(-1)^{(p-1)/2}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right).$$

因此，$\left(\frac{-3}{p}\right)=1$ 即 $\left(\frac{p}{3}\right)=1$，亦即 $p=6k+1$。这就证明了必要性。

*充分性*①　由$\left(\frac{-3}{p}\right)=1$ 知同余方程

$$s^2\equiv-3 \pmod p \tag{18}$$

必有解，设 s_0 为其解。考虑集合

$$s_0v-u,\qquad 0\leqslant u<\sqrt{p},\ 0\leqslant v<\sqrt{p}. \tag{19}$$

这集合的元素个数等于$([\sqrt{p}]+1)^2>p$，因此，由鸽巢原理知，必有两组不同的$\{u_1, v_1\}, \{u_2, v_2\}$使得

$$s_0v_1-u_1\equiv s_0v_2-u_2 \pmod p,$$

即有

$$\bar{u}\equiv s_0\bar{v} \pmod p,$$

这里 $\bar{u}=u_1-u_2$，$\bar{v}=v_1-v_2$ 一定不全为零。由此及 s_0是同余方程(18)的解可得

$$\bar{u}^2+3\bar{v}^2\equiv0 \pmod p.$$

---

① 充分性的证明所用的方法与定理1不同，这里要简单，定理1的充分性也可以这样证，请读者自己补出。

另一方面，由式(19)可得

$$0<\bar{u}^2+3\bar{v}^2<4p.$$

由以上两式推出仅有以下几种可能：

$$\bar{u}^2+3\bar{v}^2=p, 2p, 或 3p.$$

若 $\bar{u}^2+3\bar{v}^2=p$，就直接推出不定方程(17)有解；若 $\bar{u}^2+3\bar{v}^2=2p$，则必有 $2|\bar{u}+\bar{v}$，所以 $4|\bar{u}^2+3\bar{v}^2$(为什么)，因而得 $2|p$，这不可能；若 $\bar{u}^2+3\bar{v}^2=3p$，则 $3|\bar{u}$，因而有

$$\bar{v}^2+3(\bar{u}/3)^2=p,$$

这也推出不定方程(17)有解。这就证明了充分性。证毕。

习 题 二

1．找出1—99中哪些可表为两平方数之和，哪些不能。

2．若素数 $p=a^2+b^2$，那么这种表法实际上是唯一的．即假定 $a\geqslant b>0$，若还有 $p=a_1^2+b_1^2$，$a_1\geqslant b_1>0$，则必有 $a=a_1$，$b=b_1$。

3．求出(i) 5·13，(ii) 17·29，(iii) 37·41，(iv) 5·13·17·29，(v) 7^2·13·17的表为两平方数之和的所有可能的表示法。

4．若 n 及 nm 均为两平方数之和，那么，m 也是两平方数之和。

5．证明：如果一个正整数不是两个平方数之和，那么，也一定不是两个有理数的平方和。

6．证明：(i) 设 $l>0$，$m>0$。那么，有理数 l/m 是两个有理数的平方和的充要条件是 lm 为两整数的平方和；

(ii) 当(i)中的 $(l,m)=1$ 时，充要条件为 l,m 均为两平方数之和。

7．设 $n=a^2+b^2$，$(a,b)=1$。证明：若 $1\leqslant m|n$，则 $m=c^2+d^2$，$(c,d)=1$。

第8—12题利用 Legendre 符号具体给出了奇素数 p 表为两平

方数之和的公式。

8. 设 p 为奇素数，$(k,p)=1$。证明：

$$\sum_{j=0}^{p-1}\left(\frac{j(j+k)}{p}\right)=-1.$$

9. 设素数 $p\equiv1 \pmod 4$，$(k,p)=1$，以及

$$S(k)=\sum_{j=0}^{p-1}\left(\frac{j(j^2+k)}{p}\right).$$

证明：(i) $S(k)$是偶数，(ii) 对任意整数 l 有

$$S(kl^2)=\left(\frac{l}{p}\right)S(k).$$

10. 设 p 为奇素数，$\left(\frac{a}{p}\right)=1,\left(\frac{b}{p}\right)=-1$。证明：$a\cdot1^2,\cdots,a\cdot((p-1)/2)^2,b\cdot1^2,\cdots,b\cdot((p-1)/2)^2$是模 p 的既约剩余系。

11. 设素数 $p\equiv1 \pmod 4$，a,b 同第10题，及$q=(p-1)/2$。证明：(i)

$$q(S(a))^2+q(S(b))^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right),$$

其中 $S(k)$的定义同第 9 题。

(ii)

$$\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right)=\begin{cases}-2\left(\frac{xy}{p}\right), & y^2\not\equiv x^2 \pmod p,\\ (p-2)\left(\frac{xy}{p}\right), & y^2\equiv x^2 \pmod p.\end{cases}$$

(iii) $p=\left(\frac{1}{2}S(a)\right)^2+\left(\frac{1}{2}S(b)\right)^2$.

12. 利用第11题的方法，具体求出 $p=41,53,71$ 的两平方数之和的表达式。

13. 设 p 为奇素数。证明：不定方程 $p=x^2+2y^2$ 有解的充

要条件是$\left(\frac{-2}{p}\right)=1$，即 $p\equiv 1$，或 3(mod 8)。

14 设奇素数 $p>5$。以下结论正确吗：不定方程$p=x^2+5y^2$有解的充要条件是$\left(\frac{-5}{p}\right)=1$。§2定理 4 的证明方法在这里可用吗？为什么？

15. 设d,x_1,y_1,x_2,y_2都是整数。证明：存在整数 x,y满足：

$$(x_1^2-dy_1^2)(x_2^2-dy_2^2)=x^2-dy^2.$$

16. (i) 如果正整数 n 的素因数 p 都满足$\left(\frac{-3}{p}\right)=1$，则 $n=x^2+3y^2$。

(ii) 如果 n 的素因数都满足 $\left(\frac{-2}{p}\right)=1$，则 $n=x^2+2y^2$。自己找几个具体正整数 n（有两个或两个以上素因数）验证结论(i)和(ii)。

17. 第 2 题可推广如下。设 a,b 是给定两个正整数，不同时为 1，p 为素数。若 $p=ax^2+by^2$，$(x,y)=1$，$x>0$，$y>0$，有解，则解是唯一的（提示：$(ax^2+by^2)(au^2+bv^2)=(axu\pm byv)^2+ab(xv\mp yu)^2$）。

18. 设 p 是素数，$p>3$。证明：当且仅当$p\equiv 1$ (mod 6)时，不定方程 $x^2-xy+y^2=p$ 有解。

19. 设素数 $p\equiv 1$ (mod 6)。证明：必有整数 u,v 满足

$$4p=u^2+27v^2,\qquad u\equiv 1\ (\mathrm{mod}\ 3).$$

（提示：

$$\begin{aligned}4(a^2-ab+b^2)&=(a+b)^2+3(a-b)^2\\&=(2a-b)^2+3b^2=(2b-a)^2+3a^2.\end{aligned}$$）

§3* $x^2+y^2=n$ (B)

本节要证明下面的结论。

定理1 设$n\geqslant 1$. 不定方程

$$x^2+y^2=n \tag{1}$$

的解数

$$N(n)=4\sum_{d\mid n}h(d), \tag{2}$$

其中算术函数$h(d)$定义如下：$h(1)=1$,

$$h(d)=\begin{cases}0, & 2\mid d,\\(-1)^{(d-1)/2}, & 2\nmid d,\end{cases} \tag{3}$$

以及（1）的两组解$\{x_1,y_1\}$, $\{x_2,y_2\}$看作是不同的，只要$x_1\neq x_2$或$y_1\neq y_2$有一个成立。

我们将分若干个引理来证明定理1. 首先，引进几个符号和术语。不定方程（1）的解x,y称为是本原的，如果满足$(x,y)=1$；以$P(n)$表示不定方程（1）的全部非负本原解的个数；以$Q(n)$表示不定方程（1）的全部本原解的个数。

引理2 我们有

$$N(1)=Q(1)=4,\qquad P(1)=2,\qquad P(2)=1, \tag{4}$$

$$Q(n)=4P(n),\qquad n>1, \tag{5}$$

以及

$$N(n)=\sum_{d^2\mid n}Q\left(\frac{n}{d^2}\right),\qquad n\geqslant 1. \tag{6}$$

证 当$n=1$时，不定方程（1）的全部解是

$$\{\pm 1,0\},\qquad \{0,\pm 1\};$$

$n=2$时全部解是

$$\{\pm 1,\pm 1\}.$$

由此就推出式（4）. 不定方程（1）的本原解x,y必满足

$$(x,y)=(n,xy)=1. \tag{7}$$

因此，当$n>1$时，必有

$$|x|\geqslant 1,\qquad |y|\geqslant 1,$$

且$|x|,|y|$是（1）的非负本原解．所以，$n>1$时，不定方程（1）的非负本原解x_1,y_1一定是正的，且$\pm x_1,\pm y_1$给出了（1）的四组不同的本原解．这就证明了式（5）．最后，来证式（6）．设x,y是（1）的解，$(x,y)=d$．那么，必有$d^2|n$，以及$u=x/d,v=y/d$是

$$u^2+v^2=n/d^2 \tag{8}$$

的本原解，且不同的解$\{x,y\}$对应于不同的解$\{u,v\}$．反过来，设$d\geqslant 1,d^2|n$．若u,v是（8）的一组本原解，那么，$x=du,y=dv$是（1）的解，且不同的解$\{u,v\}$对应于不同的解$\{x,y\}$．这就证明了式（6）．证毕．

引理3　设$n>1$．那么，对不定方程（1）的每一组本原解x，y，必有s满足

$$sy\equiv x(\bmod n),\qquad s^2\equiv -1(\bmod n). \tag{9}$$

此外，若$\{x_1,y_1\},\{x_2,y_2\}$是（1）的两组不同的非负本原解，s_1，s_2分别是对应于它们的满足式（9）的解，那么必有

$$s_1\not\equiv s_2(\bmod n). \tag{10}$$

证　由于本原解必满足式（7），所以一次同余方程$ys\equiv x(\bmod n)$对模n必有唯一解s．进而有

$$s^2y^2\equiv x^2\equiv -y^2(\bmod n).$$

由此及$(y,n)=1$即得$s^2\equiv -1(\bmod n)$．这就证明了前半部分．当$n>1$时，由式（7）知非负本原解一定是正的，且$\neq\sqrt{n}$（为什么）．所以，

$$1\leqslant x_1,y_1<\sqrt{n},\qquad 1\leqslant x_2,y_2<\sqrt{n}.$$

因此有

$$1\leqslant x_1y_2,x_2y_1<n. \tag{11}$$

若$s_1\equiv s_2(\bmod n)$，则由$s_jy_j\equiv x_j(\bmod n)(j=1,2)$，及$(s_1s_2,n)=1$推出

$$s_1y_1x_2\equiv s_1y_2x_1(\bmod n),$$

$$y_1x_2\equiv y_2x_1(\bmod n).$$

由此及式（11）得

$$y_1x_2 = y_2x_1.$$

利用$(x_1,y_1)=(x_2,y_2)=1$，从上式及x_j,y_j均为正就推出$x_1=x_2$，$y_1=y_2$。这就证明了后半部分。证毕。

引理4 设$m>1$，$(a,m)=1$。那么，二元一次同余方程

$$au+v\equiv 0 \pmod{m} \tag{12}$$

必有解u_0,v_0，满足

$$0<|u_0|\leqslant\sqrt{m},\qquad 0<|v_0|<\sqrt{m}. \tag{13}$$

证 考虑集合$au+v$，u的取值范围是：

$$0\leqslant u\leqslant\sqrt{m}, \tag{14}$$

v的取值范围是：

$$\begin{cases}0\leqslant v<\sqrt{m}, & 当m不是平方数；\\ 0\leqslant v\leqslant\sqrt{m}-1, & 当m是平方数。\end{cases} \tag{15}$$

这样，这个集合的元素个数

$$K=\begin{cases}([\sqrt{m}]+1)^2>m, & 当m不是平方数；\\ \sqrt{m}(\sqrt{m}+1)>m, & 当m是平方数。\end{cases}$$

因此，由鸽巢原理知，必有两组不同的$\{u_1,v_1\}$，$\{u_2,v_2\}$使得

$$au_1+v_1\equiv au_2+v_2 \pmod{m}.$$

现取$u_0=u_1-u_2$，$v_0=v_1-v_2$。显见，u_0,v_0不同时为零且满足式（12）。由式（14）知，$|u_0|\leqslant\sqrt{m}$，由式（15）知，$|v_0|<\sqrt{m}$。此外，若$u_0=0$，则$v_0\neq0$。但由u_0,v_0满足式（12）推出$m|v_0$，因此$|v_0|\geqslant m$，但这和$|v_0|<\sqrt{m}$矛盾。所以$u_0\neq0$。若$v_0=0$，则$u_0\neq0$。进而由u_0,v_0满足式（12）及$(a,m)=1$推出$m|u_0$，因此$|u_0|\geqslant m$，但这和$|u_0|\leqslant\sqrt{m}$，$m>1$矛盾。所以$v_0\neq0$。引理证毕。

显见，应有$0<u_0<\sqrt{m}$（为什么）。

引理5 设$n>1$。若二次同余方程

$$s^2\equiv -1 \pmod{n} \tag{16}$$

有解 $s_1 \bmod n$，那么，不定方程（1）有本原解，且必有一组非负本原解 x_1, y_1 满足

$$s_1 y_1 \equiv x_1 \pmod n. \tag{17}$$

证　显然有 $(s_1, n) = 1$。因而由引理 4 知，必有 u_0, v_0 满足

$$0 < |u_0| \leqslant \sqrt{n}, \qquad 0 < |v_0| < \sqrt{n}, \tag{18}$$

以及

$$s_1 u_0 \equiv v_0 \pmod n. \tag{19}$$

由式（18）得

$$2 \leqslant u_0^2 + v_0^2 < 2n.$$

由 s_1 满足同余方程（16），从式（19）可推出

$$u_0^2 + v_0^2 \equiv 0 \pmod n.$$

由以上两式即得

$$u_0^2 + v_0^2 = n, \tag{20}$$

即 u_0, v_0 是（1）的解。下面来证它是本原的，即 $d = (u_0, v_0) = 1$。由式（20）得 $d^2 | n$，及由式（19）得

$$s_1(u_0/d) \equiv v_0/d \pmod{n/d}.$$

因而有

$$\frac{n}{d^2} = \left(\frac{u_0}{d}\right)^2 + \left(\frac{v_0}{d}\right)^2 \equiv \left(\frac{u_0}{d}\right)^2 + s_1^2\left(\frac{u_0}{d}\right)^2 \equiv 0\left(\bmod\ \frac{n}{d}\right),$$

这里用到了 $s_1^2 \equiv -1 \pmod{n/d}$。而上式仅当 $d = 1$ 才成立。所以，u_0, v_0 是（1）的本原解。

最后，当 u_0, v_0 同号时，取 $y_1 = |u_0|, x_1 = |v_0|$；当 u_0, v_0 异号时，取 $x_1 = |u_0|, y_1 = |v_0|$，我们不难验证 x_1, y_1 是（1）的非负（实际上是正的）本原解，且满足式（17）（留给读者）。引理证毕。

由引理 3 及引理 5 立即推出：当 $n > 1$ 时，不定方程（1）的非负（实际上一定是正的）本原解 x_1, y_1 和同余方程（16）的解

$s_1 \bmod n$之间，通过关系式（17）可建立一一对应的关系。因而它们的解数相等。以$R(n)$表示同余方程（16）的解数，这就证明了

$$P(n) = R(n), \quad n>1. \tag{21}$$

由于$R(1)=1$，$Q(1)=4$，由此及式（5），（21）就得到

$$Q(n) = 4R(n), \quad n\geqslant 1. \tag{22}$$

关于$R(n)$有下面的结论：

引理6 我们有$R(1)=1$，

$$R(2)=1, \quad R(2^{\alpha})=0, \quad \alpha>1, \tag{23}$$

以及对奇素数p有

$$R(p^{\alpha}) = 1+\left(\frac{-1}{p}\right) = \begin{cases} 2, & p\equiv 1 \pmod 4, \\ 0, & p\equiv 3 \pmod 4, \end{cases} \quad \alpha\geqslant 1. \tag{24}$$

进而，若

$$n = 2^{\alpha_0} p_1^{\alpha_1}\cdots p_r^{\alpha_r} q_1^{\beta_1}\cdots q_t^{\beta_t},$$

其中p_j, q_j是不同的奇素数且满足$p_j\equiv 1 \pmod 4$，$1\leqslant j\leqslant r$，$q_j\equiv 3 \pmod 4$，$1\leqslant j\leqslant t$，则有

$$R(n) = \begin{cases} 2^r, & \text{当}\alpha_0\leqslant 1, \ t=0, \\ 0, & \text{当}\alpha_0\geqslant 2 \ \text{或} \ t\geqslant 1. \end{cases} \tag{25}$$

证 $R(1)=1$及式（23）容易直接验证。由第四章§5推论3及定理1推出式（24）当$\alpha=1$时成立。进而，由于

$$2s\equiv 0 \pmod p$$

与同余方程（16）（$n=p$）无公共解，从第四章§4推论4就推出式（24）对$\alpha\geqslant 1$均成立。

最后，由第四章§4定理1知

$$R(n) = R(2^{\alpha_0})R(p_1^{\alpha_1})\cdots R(p_r^{\alpha_r})R(q_1^{\beta_1})\cdots R(q_t^{\beta_t}), \tag{26}$$

由此及式（23），（24），就推得式（25）。证毕。

定理1的证明 由式（6）及（22）得

$$N(n)=4\sum_{d^2\mid n}R\left(\frac{n}{d^2}\right). \tag{27}$$

设 $n=n_1n_2,(n_1,n_2)=1$. 若$d^2\mid n$, 那么,必有$(d^2,n_1)=d_1^2,(d^2,n_2)=d_2^2$, $d=d_1d_2$①; 反过来,若$d_1^2\mid n_1,d_2^2\mid n_2,d=d_1d_2$, 则$d^2\mid n$. 因此, 当$n=n_1n_2,(n_1,n_2)=1$时, 有(利用第四章§4定理1)

$$\sum_{d^2\mid n}R\left(\frac{n}{d^2}\right)=\sum_{d_1^2\mid n_1}R\left(\frac{n_1}{d_1^2}\right)\sum_{d_2^2\mid n_2}R\left(\frac{n_2}{d_2^2}\right). \tag{28}$$

设$n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, p_j是不同的素数. 由上式即得

$$\sum_{d^2\mid n}R\left(\frac{n}{d^2}\right)=\sum_{d_1^2\mid p_1^{\alpha_1}}R\left(\frac{p_1^{\alpha_1}}{d_1^2}\right)\cdots\sum_{d_r^2\mid p_r^{\alpha_r}}R\left(\frac{p_r^{\alpha_r}}{d_r^2}\right). \tag{29}$$

设 p 是素数, 我们利用引理 6 来计算(注意式(27))

$$\sum_{d^2\mid p^\alpha}R\left(\frac{p^\alpha}{d^2}\right)=\frac{1}{4}N(p^\alpha). \tag{30}$$

当$p=2$时,

$$\frac{1}{4}N(2^\alpha)=R(2^\alpha)+R(2^{\alpha-2})+\cdots+R(2^{\alpha-2[\alpha/2]})=1. \tag{31}$$

当 $p\equiv1\pmod 4$时,

$$\frac{1}{4}N(p^\alpha)=R(p^\alpha)+R(p^{\alpha-2})+\cdots+R(p^{\alpha-2[\alpha/2]})=\alpha+1. \tag{32}$$

当$p\equiv3\pmod 4$时,

$$\frac{1}{4}N(p^\alpha)=R(p^\alpha)+R(p^{\alpha-2})+\cdots+R(p^{\alpha-2[\alpha/2]})$$
$$=\begin{cases}1, & 2\mid\alpha,\\ 0, & 2\nmid\alpha.\end{cases} \tag{33}$$

① 这里的n,n_1,n_2,d,d_1,d_2均为正整数.

利用式(3)定义的 $h(d)$，从以上三式不难推得，对任意素数 p 有

$$\frac{1}{4}N(p^{\alpha})=h(1)+h(p)+\cdots+h(p^{\alpha})$$

$$=\sum_{d\mid p^{\alpha}}h(d),\qquad \alpha\geqslant 1. \tag{34}$$

由此及式（27），(29)，(30)，就得到

$$\frac{1}{4}N(n)=\left(\frac{1}{4}N(p_1^{\alpha_1})\right)\cdots\left(\frac{1}{4}N(p_r^{\alpha_r})\right)$$

$$=\left(\sum_{d_1\mid p_1^{\alpha_1}}h(d_1)\right)\cdots\left(\sum_{d_r\mid p_r^{\alpha_r}}h(d_r)\right). \tag{35}$$

由 $h(d)$ 的定义不难验证：对任意的 d,d' 有

$$h(dd')=h(d)h(d'). \tag{36}$$

由此及上式（为什么）即得

$$\frac{1}{4}N(n)=\sum_{d\mid n}h(d).$$

这就证明了式（2）。证毕。

由定理 1 立即得到

推论7 正整数 n 表为两个整数的平方和的表法个数等于 n 的 $4k+1$ 形式的正除数的个数与 $4k+3$ 形式的正除数的个数之差的四倍，进而推出，任一正整数的形如 $4k+1$ 的正除数个数一定不小于它的形如 $4k+3$ 的正除数的个数。

习 题 三

1．利用本节的结论证明 §2 习题二的第 2 题。进而证明，当 p 用 p^{α} 代替时结论仍成立。

2．对 $n=200,201,202,203$ 计算 $N(n)$，$P(n)$ 和 $Q(n)$。

3．证明：当 n 没有大于 1 的平方因数时，$N(n)=Q(n)$，解释本题的意义。

4．直接证明任一正整数 n 的形如 $4k+1$ 的正除数个数不少于形如$4k+3$的正除数的个数。

5．求 $Q(n)=0$的充要条件。

6．设$1<n\equiv1 \pmod 4$。以$N^*(n)$，$P^*(n)$及$Q^*(n)$分别表示不定方程$4x^2+y^2=n$ 的全部解的个数，非负的本原解的个数，及全部本原解的个数，这里本原解是指 $(x,y)=1$。证明：

$$N^*(n)=N(n)/2,\quad P^*(n)=P(n)/2,\quad 及\ Q^*(n)=Q(n)/2.$$

7．设$1<n\equiv1 \pmod 4$。在第 6 题的意义下，证明：

(i) 若 n 是素数，则不定方程 $4x^2+y^2=n$ 恰有一组非负解，而且一定是本原的。

(ii) 若 n 是合数，则不定方程 $4x^2+y^2=n$，要么没有本原解或有多于一组本原解；要么有一组非负本原解，且同时还至少有一组非负的非本原解。

8．设$1<n\equiv1 \pmod 4$是给定的正整数。证明我们可用下面方法来缩小$4x^2+y^2=n$的非负解x,y 的范围：(i) $0\leqslant x\leqslant\sqrt{n}/2$；(ii) 取定奇素数 q 及模 q 的二次非剩余a，$-4x^2\not\equiv a-n \pmod q$；(iii) 当$n\equiv1 \pmod 8$时，$2|x$。以$n=4993$为例，取$q=5, a=2,3$，证明：$x$ 仅可能在 $4,6,14,24,26,34$ 中取值。若再取 $q=7$，$a=3,5,6$，则可推出 x 不能取值 $14,34$。由此推出，仅有非负解 $x=16, y=63$。进而，由第 7 题证明4993 是素数。这里实际上给出了正整数$n\equiv1 \pmod 4$ 的一个素性判别法。

9．利用第 8 题方法，判断 $n=5209,5429,6101,5809$ 是不是素数。

10．设$N_4(n)$表示 $n=x_1^2+x_2^2+x_3^2+x_4^2$ 的全部解数（次序不同，正负号不同均看作不同的解），$\sigma(n)$表示 n 的正除数之和，即$\sigma(n)=\sum\limits_{d|n} d$（例如，$\sigma(6)=1+2+3+6=12$）。本题是利用对$x^2+y^2=n$的全部解数$N(n)$的讨论与结论来证明：

$$N_4(n)=\begin{cases}8\sigma(n), & 2\nmid n,\\ 24\sigma(m), & n=2^km, k\geqslant1, 2\nmid m.\end{cases}$$

(i) 设$2\nmid n$，$M(n)$是不定方程 $4n=u_1^2+u_2^2+u_3^2+u_4^2$，$2\nmid u_j$ $(1\leqslant j\leqslant 4)$的全部解数。证明：$M(n)=\sigma(n)$；

(ii) 设 $2\nmid n$。证明：$N_4(2n)=3N_4(n)$，$N_4(2n)=N_4(4n)$，及$N_4(4n)=16\sigma(n)+N_4(n)$；

(iii) 由(i)，(ii)推出所要结论；

(iv) 对 $n=105,210$ 验证以上结论的正确性（提示：为证(i)利用

$$M(n)=\sum_{a+b=2n}\frac{N(2a)}{4}\frac{N(2b)}{4}$$

$$=\sum_{a+b=2n}\left(\sum_{s\mid 2a}h(s)\right)\left(\sum_{t\mid 2b}h(t)\right)$$

$$=\sum_{sx-ty=2n}h(st).$$

这里变数 s,t,x,y 取正奇数。把最后和式分$s=t$和 $s\neq t$ 两部分讨论，$s=t$的这一部分之和等于$\sigma(n)$，另一部分为零）。

§ 4* $ax^2+by^2+cz^2=0$

这一节要讨论不定方程

$$ax^2+by^2+cz^2=0,\qquad x,y,z\text{不全为零}. \tag{1}$$

我们将证明如下结论：

定理1 设 a,b,c 均是非零整数，且乘积 abc 无平方因数，那么，不定方程(1)有解的充要条件是：a,b,c 的正负号不全相同，以及 $-bc$，$-ca$，$-ab$ 分别是模 a,b,c 的二次剩余，即二次同余方程

$$s^2\equiv -bc\pmod{|a|}, \tag{2}$$

$$s^2\equiv -ca\pmod{|b|}, \tag{3}$$

及

$$s^2\equiv -ab\pmod{|c|} \tag{4}$$

均有解。

先来证明两个引理。

引理2　设 m 是正整数，α,β,γ 是正实数满足 $\alpha\beta\gamma=m$。那么，对任意整数 d,e,f，同余方程

$$dx+ey+fz\equiv 0\pmod{m} \tag{5}$$

必有一组不全为零的解 x_1,y_1,z_1，满足

$$|x_1|\leqslant\alpha,\ |y_1|\leqslant\beta,\ |z_1|\leqslant\gamma. \tag{6}$$

证　考虑整数集合：$du+ev+fw,\ 0\leqslant u\leqslant\alpha,\ 0\leqslant v\leqslant\beta,\ 0\leqslant w\leqslant\gamma$。这一集合的元素个数等于

$$(1+[\alpha])(1+[\beta])(1+[\gamma])>\alpha\beta\gamma=m.$$

因此，必有不同的两组 $\{u_1,v_1,w_1\},\{u_2,v_2,w_2\}$ 使得

$$du_1+ev_1+fw_1\equiv du_2+ev_2+fw_2\pmod{m}.$$

取 $x_1=u_1-u_2,\ y_1=v_1-v_2,\ z_1=w_1-w_2$，就满足引理要求。证毕。

引理3　设 $(m_1,m_2)=1$。若

$$\begin{aligned}&ax^2+by^2+cz^2\\&\quad\equiv(d_1x+e_1y+f_1z)(d_1'x+e_1'y+f_1'z)\pmod{m_1},\\&ax^2+by^2+cz^2\\&\quad\equiv(d_2x+e_2y+f_2z)(d_2'x+e_2'y+f_2'z)\pmod{m_2},\end{aligned}$$

那么，必有 d,e,f,d',e',f'，使得

$$\begin{aligned}&ax^2+by^2+cz^2\\&\quad\equiv(dx+ey+fz)(d'x+e'y+f'z)\pmod{m_1m_2},\end{aligned}$$

这里的同余式均为恒等同余式，即对任意整数 x,y,z 都成立。

证　由孙子定理（第四章§3定理1）知，一定存在 d,e,f,d',e',f' 满足

$$d\equiv d_j\pmod{m_j},\ e\equiv e_j\pmod{m_j},\ f\equiv f_j\pmod{m_j},\ j=1,2,$$

$$d'\equiv d_j'\pmod{m_j},\ e'\equiv e_j'\pmod{m_j},\ f'\equiv f_j'\pmod{m_j},\ j=1,2.$$

因而有

$$\begin{aligned}&ax^2+by^2+cz^2\\&\quad\equiv(dx+ey+fz)(d'x+e'y+f'z)\pmod{m_j},\quad j=1,2.\end{aligned}$$

由此即得所要的结论.

定理1的证明 由条件abc无平方因数可推出a,b,c两两既约.

必要性 设不定方程(1)有解x_1,y_1,z_1. 显见a,b,c不能有相同的符号. 不妨设$(x_1,y_1,z_1)=1$（为什么）. 我们来证明同余方程(2)有解. 为此, 先证必有$(a,z_1)=1$. 若不然, 必有素数$p|a$, $p|z_1$. 因而$p|by_1^2$, 由于$(a,b)=1$, $p\nmid b$, 所以$p|y_1$. 因此有$p^2|ax_1^2$, 由于a无平方因数, 故得$p|x_1$, 但这和$(x_1,y_1,z_1)=1$矛盾. 因而有z_1^{-1}满足$z_1z_1^{-1}\equiv1(\bmod|a|)$, 由此得

$$by_1^2\equiv-cz_1^2(\bmod |a|),$$
$$(by_1z_1^{-1})^2\equiv-bc(\bmod |a|),$$

这就证明了（2）有解. 由对称性就推出同余方程（3）及（4）也有解.

充分性 由$(a,b)=1$及（2）有解知, 存在s_1及b^{-1}满足$s_1^2\equiv-bc(\bmod |a|)$及$bb^{-1}\equiv1(\bmod |a|)$. 这样, 就有恒等同余式

$$\begin{aligned}by^2+cz^2&\equiv bb^{-1}(by^2+cz^2)\equiv b^{-1}(b^2y^2+bcz^2)\\&\equiv b^{-1}(b^2y^2-s_1^2z^2)\\&\equiv b^{-1}(by-s_1z)(by+s_1z)\\&\equiv(y-b^{-1}s_1z)(by+s_1z)(\bmod |a|).\end{aligned}$$

进而有

$$ax^2+by^2+cz^2\equiv(y-b^{-1}s_1z)(by+s_1z)(\bmod |a|). \tag{7}$$

类似可得恒等同余式

$$ax^2+by^2+cz^2\equiv(z-c^{-1}s_2x)(cz+s_2x)(\bmod |b|), \tag{8}$$
$$ax^2+by^2+cz^2\equiv(x-a^{-1}s_3y)(ax+s_3y)(\bmod |c|), \tag{9}$$

其中s_2,s_3分别满足同余方程（3）,（4）以及$cc^{-1}\equiv1(\bmod |b|)$, $aa^{-1}\equiv1(\bmod |c|)$. 由以上三式, 两次利用引理3, 就推出存在整数d,e,f,d',e',f', 使有恒等同余式

$$ax^2+by^2+cz^2$$

$$\equiv (dx+ey+fz)(d'x+e'y+f'z)\pmod{|abc|} \quad (10)$$

成立。上式称为 $ax^2+by^2+cz^2$ 对模 abc 可分解为一次式的乘积。

为使讨论确定起见，可以假定 $a>0, b<0, c<0$。因为以 $-a$, $-b$, $-c$ 代 a,b,c 后，不定方程(1)及定理 1 的条件均不变，所以，由此及 a,b,c 正负号不全相同知，可假设它们是一正、两负。因而（必要时改变字母 a,b,c 的记号）可作所说的假定。

现在应用引理 2 来讨论同余方程

$$dx+ey+fz\equiv 0\pmod{abc}. \quad (11)$$

取 $\alpha=\sqrt{bc}$, $\beta=\sqrt{|ca|}$, $\gamma=\sqrt{|ab|}$，由引理 2 知，同余方程（11）必有一组不全为零的解 x_1, y_1, z_1，满足

$$|x_1|\leqslant\sqrt{bc}, \quad |y_1|\leqslant\sqrt{|ca|}, \quad |z_1|\leqslant\sqrt{|ab|}. \quad (12)$$

由于 abc 无平方因数，上面等号分别仅当 $bc=1, |ca|=1, |ab|=1$ 才有可能成立。因为 a 是正的，b,c 是负的，所以，除了

$$b=c=-1 \quad (13)$$

外，必有

$$ax_1^2+by_1^2+cz_1^2\leqslant ax_1^2<abc,$$
$$ax_1^2+by_1^2+cz_1^2\geqslant by_1^2+cz_1^2$$
$$>b(-ac)+c(-ab)=-2abc.$$

由式（10）知，

$$ax_1^2+by_1^2+cz_1^2\equiv 0\pmod{abc}.$$

因此，当式（13）不成立时必有

$$ax_1^2+by_1^2+cz_1^2=0 \text{ 或 } -abc.$$

当上式第一种情形成立时，我们就找到了不定方程（1）的一组解 x_1, y_1, z_1。当第二种情形成立时，取

$$x_2=-by_1+x_1z_1, \quad y_2=ax_1+y_1z_1, \quad z_2=z_1^2+ab,$$

容易验证

$$ax_2^2+by_2^2+cz_2^2=0.$$

当 x_2, y_2, z_2 不全为零时，也得到了不定方程(1)的一组解 x_2, y_2, z_2。

当 $x_2=y_2=z_2=0$ 时，我们有 $z_1^2=-ab$，由于 ab 无平方因数，所以必有 $a=1, b=-1$（注意对 a,b,c 的正负号假定）。因而 $x=1$，$y=1, z=0$ 是不定方程(1)的解。

最后来讨论式（13）成立的特殊情形。这时（1）变为

$$y^2+z^2=ax^2,\quad x,y,z\text{不全为零}. \tag{14}$$

由条件知 -1 是模 a 的二次剩余。因此，由§2定理3（并利用第四章§5推论3）或§3式（22）均可推出不定方程

$$\bar{y}^2+\bar{z}^2=a,\quad (\bar{y},\bar{z})=1$$

有解 $\bar{y}_1,\bar{z}_1$。这样，$x=1, y=\bar{y}_1, z=\bar{z}_1$，就是（14），即（1）的一组解。证毕。

例1 判断以下不定方程是否有不全为零的解，有解时求出它的一组解：

（i）$5x^2-14y^2-41z^2=0$；（ii）$3x^2-14y^2-19z^2=0$。

解 （i）这时 $a=5, b=-14, c=-41$。由定理1知，只要验证同余方程（2），（3），（4）是否都有解。我们有

$$s^2\equiv-(-14)\cdot(-41)\equiv1 \pmod 5,$$

所以（2）有解；

$$s^2\equiv-(-41)\cdot(5)\equiv-5\equiv3^2 \pmod{14},$$

所以（3）有解；最后，我们有

$$s^2\equiv-(5)\cdot(-14)\equiv-12 \pmod{41}.$$

41是素数，我们计算Legendre符号

$$\left(\frac{-12}{41}\right)=\left(\frac{-1}{41}\right)\left(\frac{2^2}{41}\right)\left(\frac{3}{41}\right)$$

$$=\left(\frac{3}{41}\right)=\left(\frac{41}{3}\right)=\left(\frac{-1}{3}\right)=-1,$$

所以，(4)无解。因此不定方程（i）无不全为零的解。

（ii）这里 $a=3, b=-14, c=-19$。由定理1知，也先要验证同余方程（2），(3)，(4）是否都有解。我们有

$$s^2 \equiv -(-14)\cdot(-19) \equiv 1 \pmod 3,$$

所以(2)有解；

$$s^2 \equiv -(-19)\cdot(3) \equiv 1 \pmod{14},$$

所以(3)有解；以及

$$s^2 \equiv -3\cdot(-14) \equiv 2^2 \pmod{19},$$

所(4)亦有解。为了具体找出(ii)的一个解，从定理1的充分性证明知，先要把$ax^2+by^2+cz^2$对模a,b,c分别分解为两个一次式的乘积。当然可以按证明方法来做，但在简单的具体问题中可以直接分解。我们有：

$$-14y^2-19z^2 \equiv y^2-z^2 \equiv (y-z)(y+z) \pmod 3;$$

$$\begin{aligned}3x^2-19z^2 &\equiv 5(9x^2-57z^2) \equiv 5(9x^2-z^2)\\ &\equiv 5(3x-z)(3x+z)\\ &\equiv (x-5z)(3x+z) \pmod{14};\end{aligned}$$

$$\begin{aligned}3x^2-14y^2 &\equiv -6(9x^2-42y^2) \equiv -6(9x^2-4y^2)\\ &\equiv -6(3x-2y)(3x+2y)\\ &\equiv (x-7y)(3x+2y) \pmod{19}.\end{aligned}$$

进而有(相应于式(7),(8)及(9))

$$\begin{cases}3x^2-14y^2-19z^2 \equiv (y-z)(y+z) \pmod 3,\\ 3x^2-14y^2-19z^2 \equiv (x-5z)(3x+z) \pmod{14},\\ 3x^2-14y^2-19z^2 \equiv (x-7y)(3x+2y) \pmod{19}.\end{cases} \tag{15}$$

我们当然可以如同在充分性证明中所做的那样去求出相应的分解式(10)，然后去求同余方程满足条件(12)的解(这一做法留给读者)。但在具体的数值题中我们可以直接去求解下述同余方程组的解(为什么)：

$$\begin{cases}y-z \equiv 0 \pmod 3,\\ x-5z \equiv 0 \pmod{14},\\ x-7y \equiv 0 \pmod{19},\\ |x| \leqslant [\sqrt{14\cdot 19}] = 16,\\ |y| \leqslant [\sqrt{3\cdot 19}] = 7,\\ |z| \leqslant [\sqrt{3\cdot 14}] = 6.\end{cases} \tag{16}$$

由取值范围最小的变数z开始具体取值试算，可得$z_1=-1$，$y_1=2$，$x_1=-5$是解。这时

$$3\cdot(-5)^2-14\cdot(2)^2-19\cdot(-1)^2=75-56-19=0.$$

所以，这是不定方程(ii)的一组解。如果在试算中，我们得到了(16)的这样一组解：$z_1=5$，$y_1=5$，$x_1=-3$。这时

$$3\cdot(-3)^2-14\cdot5^2-19\cdot5^2=-798=-3\cdot(-14)\cdot(-19).$$

由充分性证明中的讨论知，应取

$$x_2=-(-14)\cdot5+(-3)\cdot(5)=55,$$
$$y_2=3\cdot(-3)+5\cdot5=16,$$
$$z_2=5^2+3\cdot(-14)=-17.$$

容易验证，这就是不定方程(ii)的一组解。

应该指出，同余方程组(16)是根据式(15)得到的，它的取法显然不是唯一的。事实上，只要从式(15)的三个同余式的右边各任取定一个一次因式就可构成式(16)的同余方程组，例如，代替(16)可取

$$\begin{cases}y-z\equiv0\pmod 3,\\ 3x+z\equiv0\pmod{14},\\ 3x+2y\equiv\pmod{19},\\ |x|\leqslant16,\quad |y|\leqslant7,\quad |z|\leqslant6.\end{cases}\tag{17}$$

习　题　四

1．判断以下不定方程是否有不全为零的解。如果可解，则按定理 1 证明的途径求出它的一组解。

(i) $3x^2+7y^2-5z^2=0$；　　(ii) $5x^2-17y^2+3z^2=0$；

(iii) $19x^2-7y^2-11z^2=0$；　　(iv) $7x^2-43y^2-3z^2=0$；

(v) $4x^2+3y^2-5z^2=0$；　　(vi) $41x^2+3y^2-11z^2=0$。

2．证明定理 1 与下面的命题等价：设正整数 a,b 均无平方因数。那么，不定方程

$$ax^2+by^2=z^2,\qquad x,y,z\text{不全为零}$$

有解的充要条件是：

(i) 同余方程 $x^2\equiv a \pmod b$ 有解；

(ii) $x^2\equiv b \pmod a$ 有解；

(iii) $x^2\equiv -ab/d^2 \pmod d$ 有解，$d=(a,b)$。

3．按以下途径直接证明第 2 题中的命题：

(i) $a=1$ 时命题成立；(ii) $a=b$ 时命题成立；以下不妨假定 $a>b>1$。(iii) 存在整数 $T,c,|c|\leqslant a/2$，使得

$$c^2-b=aT=aAm^2,\qquad A,m\in \boldsymbol{Z},$$

其中 A 是无平方因子数．证明：$0<A<a$；(iv) $x^2\equiv A \pmod b$ 有解；(v) $x^2\equiv -Ab/(A,b)^2 \pmod{(A,b)}$ 有解；(vi) 不定方程 $Ax^2+by^2=z^2$ 满足命题的条件(i)，(ii)及(iii)；(vii) 若 x_0,y_0,z_0 是(vi)中的不定方程的非显然解，则 $x=Amx_0$，$y=cy_0+z_0$，$z=cz_0+by_0$ 是 $ax^2+by^2=z^2$ 的非显然解。(viii) 把命题归结为(i)或(ii)的情形。

4．设 a,b,c 是非零整数，且正负号不全相同，abc 无平方因数。证明：§4中不定方程(1)有解的充要条件是有§4中的恒等同余式(10)成立。

§5* $x^3+y^3=z^3$

本节将证明

定理1 不定方程

$$x^3+y^3=z^3 \tag{1}$$

无 $xyz\neq 0$ 的解。

这一结论的证明主要用到§2定理4及下面的引理。

引理2 设 $2\nmid s$。那么，

$$s^3=a^2+3b^2,\quad (a,b)=1 \tag{2}$$

成立的充要条件是存在 α,β 使得

$$s = \alpha^2 + 3\beta^2, \quad (\alpha, 3\beta) = 1, \tag{3}$$

及

$$a = \alpha^3 - 9\alpha\beta^2, \quad b = 3\alpha^2\beta - 3\beta^3. \tag{4}$$

证 *充分性* 设式(3)和(4)成立。为使推导清楚，利用复数运算。由式(3)知

$$s = (\alpha + \sqrt{-3}\beta)(\alpha - \sqrt{-3}\beta),$$

因而有

$$\begin{aligned} s^3 &= (\alpha + \sqrt{-3}\beta)^3(\alpha - \sqrt{-3}\beta)^3 \\ &= \{(\alpha^3 - 9\alpha\beta^2) + \sqrt{-3}(3\alpha^2\beta - 3\beta^3)\} \\ &\quad \times \{(\alpha^3 - 9\alpha\beta^2) - \sqrt{-3}(3\alpha^2\beta - 3\beta^3)\} \\ &= (\alpha^3 - 9\alpha\beta^2)^2 + 3(3\alpha^2\beta - 3\beta^3)^2. \end{aligned}$$

由此及式(4)推出 $s^3 = a^2 + 3b^2$。由 $(\alpha, 3\beta) = 1$ 可得(注意：$2 \nmid s$，$2 \nmid \alpha \pm \beta$)

$$\begin{aligned} (a, b) &= (\alpha^2 - 9\beta^2, \alpha^2 - \beta^2) = (8\beta^2, \alpha^2 - \beta^2) \\ &= (\beta^2, \alpha^2 - \beta^2) = 1. \end{aligned}$$

这就证明了式(2)成立。

必要性 设式(2)成立。这时必有 $3 \nmid s$，因此，s 的任一素因数 p 一定满足

$$p > 3, \quad (p, ab) = 1. \tag{5}$$

进而推出(为什么)必有

$$\left(\frac{-3}{p}\right) = 1. \tag{6}$$

以$\Omega(s)$记 s 的素因数个数(按重数计)，且约定$\Omega(1) = 0$。如$\Omega(6) = 2$，$\Omega(4) = 2$。我们对$\Omega(s)$用归纳法来证必要性。当$\Omega(s) = 0$即$s = 1$时，有$a = \pm 1$，$b = 0$。这时可取$\alpha = \pm 1$，$\beta = 0$。所以必要性成立，假设对 $\Omega(s) = n(\geqslant 0)$时必要性成立。当 $\Omega(s) = n + 1$时，设 $s = pt$，p 是素数，$\Omega(t) = n$。由于 p 满足式(6)，由§2定理 4 知

$$p = \alpha_1^2 + 3\beta_1^2, \tag{7}$$

且显然有

$$(\alpha_1, 3\beta_1) = 1. \tag{8}$$

由充分性的证明知

$$p^3 = c^2 + 3d^2, \quad (c, d) = 1, \tag{9}$$

$$c = \alpha_1^3 - 9\alpha_1\beta_1^2, \quad d = 3\alpha_1^2\beta_1 - 3\beta_1^3. \tag{10}$$

由此及式(2)得

$$p^6t^3 = p^3s^3 = (c^2 + 3d^2)(a^2 + 3b^2)$$

$$\begin{aligned}
&= \begin{cases} (c + \sqrt{-3}d)(a - \sqrt{-3}b)(c - \sqrt{-3}d)(a + \sqrt{-3}b), \\ (c + \sqrt{-3}d)(a + \sqrt{-3}b)(c - \sqrt{-3}d)(a - \sqrt{-3}b) \end{cases} \\
&= (ac + 3bd)^2 + 3(ad - bc)^2 \\
&= (ac - 3bd)^2 + 3(ad + bc)^2.
\end{aligned} \tag{11}$$

下面来证明：$ad - bc$ 和 $ad + bc$ 两数中有且仅有一个被 p 整除。我们有(利用式(2)和式(9))

$$\begin{aligned}(ad - bc)(ad + bc) &= (a^2 + 3b^2)d^2 - (c^2 + 3d^2)b^2 \\ &= p^3(t^3d^2 - b^2).\end{aligned} \tag{12}$$

因此，p 至少整除其中的一个数。但若 $p \mid (ad - bc, ad + bc)$，则 $p \mid (ad, bc)$(因为$p > 3$)。而由式(9)知$p \nmid cd$，所以 $p \mid (a, b)$，这和$(a, b) = 1$矛盾，这就证明了所要结论，且由式(12)知被 p 整除的数必被p^3整除。假设 $p^3 \mid ad - bc$(对 $p^3 \mid ad + bc$ 的情形可同样讨论)，由式(11)知

$$t^3 = u^2 + 3v^2, \tag{13}$$

$$u = (ac + 3bd)/p^3, \quad v = (ad - bc)/p^3. \tag{14}$$

我们来证明必有

$$(u, v) = 1. \tag{15}$$

由式(9)和(14)得

$$ac + 3bd = u(c^2 + 3d^2),$$

$$ad - bc = v(c^2 + 3d^2),$$

由此推出(分别消去 b 和 a)

$$a = uc + 3vd, \qquad b = ud - vc. \tag{16}$$

从以上两式及 $(a,b) = 1$ 就推出式(15)成立。

至此我们得到：$\Omega(t) = n$ 且有式(13)和(15)成立。因而由归纳假设知，必有 α_2, β_2 使得

$$t = \alpha_2^2 + 3\beta_2^2, \quad (\alpha_2, 3\beta_2) = 1, \tag{17}$$

及

$$u = \alpha_2^3 - 9\alpha_2\beta_2^2, \quad v = 3\alpha_2^2\beta_2 - 3\beta_2^3. \tag{18}$$

由式(7)和(17)可得(类似于式(11))

$$s = pt = (\alpha_1^2 + 3\beta_1^2)(\alpha_2^2 + 3\beta_2^2) = \alpha^2 + 3\beta^2, \tag{19}$$

这里取

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2, \quad \beta = \alpha_2\beta_1 - \beta_2\alpha_1. \tag{20}$$

这样，为了证明当 $\Omega(s) = n+1$ 时必要性成立，只要证明对所取的 α, β 式(4)成立，及 $(\alpha, 3\beta) = 1$。为使推导清楚，我们仍利用复数运算。式(16)可写为

$$a + \sqrt{-3}b = (c + \sqrt{-3}d)(u - \sqrt{-3}v).$$

式(10)可写为

$$c + \sqrt{-3}d = (\alpha_1 + \sqrt{-3}\beta_1)^3.$$

式(18)可写为

$$u - \sqrt{-3}v = (\alpha_2 - \sqrt{-3}\beta_2)^3.$$

由以上三式及式(20)可得

$$\begin{aligned} a + \sqrt{-3}b &= \{(\alpha_1\alpha_2 + 3\beta_1\beta_2) + \sqrt{-3}(\alpha_2\beta_1 - \beta_2\alpha_1)\}^3 \\ &= (\alpha + \sqrt{-3}\beta)^3. \end{aligned}$$

比较上式两边的实虚部就推出式(4)成立。由式(2)知 $(a, 3b) = 1$，由此及式(4)即得 $(\alpha, 3\beta) = 1$。证毕。

定理1的证明 用反证法。假设有 $xyz \neq 0$ 的解。设 x_0, y_0, z_0 是这样的一组解，使得 $|x_0y_0z_0|$ 取最小值。显见，必有 $(x_0, y_0, z_0) = 1$。进而推出

$$(x_0,y_0)=(y_0,z_0)=(z_0,x_0)=1.$$

所以，x_0,y_0,z_0必为两奇一偶，不妨设$2|z_0$(若y_0为偶，则$x=x_0$，$y=-z_0$，$z=-y_0$是(1)的这种解；若x_0为偶，则$x=-z_0$，$y=y_0$，$z=-x_0$是(1)的这种解)。令

$$x_0+y_0=2u_0,\quad x_0-y_0=2w_0. \tag{21}$$

显然有$u_0w_0\neq0$，若不然，必有$|x_0|=|y_0|$，由此及$(x_0,y_0)=1$推出$|x_0|=|y_0|=1$，而这时必有$z_0=0$，所以不可能。由$(x_0,y_0)=1$及$2\nmid x_0y_0$可推出(为什么)

$$2\nmid u_0\pm w_0,\quad (u_0,w_0)=1. \tag{22}$$

由式(21)得

$$\begin{aligned}z_0^3&=(u_0+w_0)^3+(u_0-w_0)^3\\&=2u_0(u_0^2+3w_0^2).\end{aligned} \tag{23}$$

以下分(i) $3\nmid u_0$，(ii) $3|u_0$两种情形来讨论。

(i) $3\nmid u_0$的情形。由式(22)知，这时有

$$(2u_0,u_0^2+3w_0^2)=1.$$

由第一章§6推论5及$u_0\neq0$知

$$0\neq2u_0=t^3,\quad u_0^2+3w_0^2=s^3.$$

由引理2知，必有α,β使得

$$s=\alpha^2+3\beta^2,\quad (\alpha,3\beta)=1,$$

$$u_0=\alpha^3-9\alpha\beta^2,\quad w_0=3\alpha^2\beta-3\beta^3.$$

所以，

$$t^3=2\alpha(\alpha-3\beta)(\alpha+3\beta)\neq0.$$

容易验证$2\alpha,\alpha-3\beta,\alpha+3\beta$两两既约，因而由第一章§6推论5知

$$2\alpha=\sigma^3,\quad \alpha-3\beta=\tau^3,\quad \alpha+3\beta=\rho^3.$$

显见，τ,ρ,σ是(1)的解，即

$$\tau^3+\rho^3=\sigma^3.$$

但这时有

$$\begin{aligned}0\neq|\sigma\tau\rho|^3&=|t|^3=|2u_0|=|x_0+y_0|\\&\leqslant|x_0^3+y_0^3|=|z_0|^3<|x_0y_0z_0|^3,\end{aligned}$$

最后一步用到了$|x_0y_0|>1$(前已指出$|x_0y_0|=1$时必有$z_0=0$，所以不可能)。因而

$$0\neq|\sigma\tau\rho|<|x_0y_0z_0|.$$

这和$|x_0y_0z_0|$的最小性矛盾。所以不可能。

(ii) $3|u_0$的情形。设$u_0=3v_0$，式(23)变为

$$z_0^3=18v_0(3v_0^2+w_0^2).$$

由式(22)知$(3v_0,w_0)=1$. $2\nmid 3v_0+w_0$，所以

$$(18v_0,3v_0^2+w_0^2)=1.$$

由第一章§6推论5知

$$0\neq 18v_0=\bar{t}^3,\quad 3v_0^2+w_0^2=\bar{s}^3.$$

由引理2知，必有$\bar{\alpha},\bar{\beta}$使得

$$\bar{s}=\bar{\alpha}^2+3\bar{\beta}^2,\quad (\bar{\alpha},3\bar{\beta})=1.$$
$$w_0=\bar{\alpha}^3-9\bar{\alpha}\bar{\beta}^2,\quad v_0=3\bar{\alpha}^2\bar{\beta}-3\bar{\beta}^3.$$

所以

$$0\neq(\bar{t}/3)^3=2\bar{\beta}(\bar{\alpha}+\bar{\beta})(\bar{\alpha}-\bar{\beta}).$$

易证$2\bar{\beta},\bar{\alpha}+\bar{\beta},\bar{\alpha}-\bar{\beta}$两两既约。因而由第一章§6推论5知

$$2\bar{\beta}=\bar{\sigma}^3,\quad \bar{\alpha}+\bar{\beta}=\bar{\tau}^3,\quad \bar{\alpha}-\bar{\beta}=\bar{\rho}^3.$$

显见，$\bar{\tau},\bar{\rho},\bar{\sigma}$是(1)的解，即

$$\bar{\tau}^3+\bar{\rho}^3=\bar{\sigma}^3.$$

但这时有

$$\begin{aligned}0\neq|\bar{\sigma}\bar{\tau}\bar{\rho}|^3&=|\bar{t}/3|^3=|2v_0/3|=|2u_0/9|\\&=|x_0+y_0|/9\leqslant|x_0^3+y_0^3|/9\\&=|z_0|^3/9<|x_0y_0z_0|^3,\end{aligned}$$

这和$|x_0y_0z_0|$的最小性矛盾。所以也不可能。定理全部证毕。

第七章* 连分数

§1 什么是连分数

连分数是一个很有用的工具。我们先来举几个例子，说明什么叫连分数以及它的用处。

例 1 如果你手边没有平方根表，也没有计算器，那么能用什么简单方法来求$\sqrt{11}$的近似值？当然可以用通常的求平方根的方法，但下面的办法看来更方便。

$$3<\sqrt{11}<4, \tag{1}$$

$$\sqrt{11}=3+(\sqrt{11}-3) \tag{2}$$

$$=3+\frac{1}{(\sqrt{11}+3)/2}$$

$$=3+\frac{1}{3+(\sqrt{11}-3)/2} \tag{3}$$

$$=3+\cfrac{1}{3+\cfrac{1}{\sqrt{11}+3}}$$

$$=3+\cfrac{1}{3+\cfrac{1}{6+(\sqrt{11}-3)}}. \tag{4}$$

重复这一过程就可得到

$$\sqrt{11}=3+\cfrac{1}{3+\cfrac{1}{6+\cfrac{1}{3+(\sqrt{11}-3)/2}}} \tag{5}$$

$$= 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + (\sqrt{11} - 3)}}}} \tag{6}$$

$$= 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + (\sqrt{11} - 3)/2}}}}} \tag{7}$$

$$= 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + (\sqrt{11} - 3)}}}}}} \tag{8}$$

$= \cdots\cdots$。

马上就会想到分别把式(2)，(3)，(4)，(5)，(6)，(7)，(8)中的无理数$(\sqrt{11}-3)$或$(\sqrt{11}-3)/2$去掉后所得到的“分数”值来作为$\sqrt{11}$的“近似值”。容易算出，这些“近似值”依次为：

$$\sqrt{11} \approx 3, \frac{10}{3}, \frac{63}{19}, \frac{199}{60}, \frac{1257}{379}, \frac{3970}{1197}, \frac{25077}{7561}. \tag{9}$$

用小数表示，这些“近似值”依次为(取八位小数)：

$$\sqrt{11} \approx 3, 3.33333333, 3.31578947, 3.31666666, 3.316622691, 3.31662489, 3.31662478. \tag{10}$$

这些的确是很精确的近似值，因为实际上

$$\sqrt{11} = 3.31662479\cdots. \tag{11}$$

若取10/3作近似值，就精确到$2/10^2$；取 63/19 就精确到 $9/10^4$；

取199/60就精确到$42/10^6$；取1257/379就精确到$22/10^7$；取3970/1197就精确到$1/10^7$；取25077/7561就精确到$1/10^8$。这些数据表明，这些近似值依次一个比一个更精确。此外，容易看出

$$3<\frac{63}{19}<\frac{1257}{379}<\frac{25077}{7561}<\sqrt{11}<\frac{3970}{1197}<\frac{199}{60}<\frac{10}{3}. \qquad (12)$$

这个例子表明，它提出了一个方法来构造一些特殊形式的"分数"，作为无理数的近似值。因而也就提出了研究这种形式"分数"的性质的新课题，以及从理论上研究无理数的这种形式的有理数逼近。另外，以上的过程不断的继续下去，就可以得到一个无穷尽的"分数"表达式：

$$3+\cfrac{1}{3+\cfrac{1}{6+\cfrac{1}{3+\cfrac{1}{6+\cfrac{1}{3+\cfrac{1}{6+\cfrac{1}{3+\cfrac{1}{6+\cdots}}}}}}}} \qquad (13)$$

这种表达式的确切含意是什么呢？能否定义它的"值"？如果能定义它的"值"，那么这"值"和$\sqrt{11}$有什么关系？这就又提出了进一步的研究课题。

例 2　一个分母、分子很大的分数用起来是很不方便的，如103993/33102。我们想找一个分母、分子较小的分数来近似它，希望分母不要太大，但误差很小。利用例 1 的方法可得

$$\frac{103993}{33102}=3+\frac{4687}{33102}=3+\cfrac{1}{7+\cfrac{293}{4687}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{292}{293}}}$$

$$=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292}}}}.$$

类似于例1，我们扔掉这些“分数”中小于1的数$\frac{4687}{33102}$，$\frac{293}{4687}$，$\frac{292}{293}$，$\frac{1}{292}$，用依次得到的

$$3,\quad 3+\frac{1}{7}=\frac{22}{7},\quad 3+\cfrac{1}{7+\cfrac{1}{15}}=\frac{333}{106},$$

$$3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}}=\frac{355}{113}$$

来近似$103993/33102=3.141592653\cdots$。由

$$\frac{22}{7}=3.14285714\cdots,\quad \frac{333}{106}=3.14150943\cdots,$$

$$\frac{355}{113}=3.14159292\cdots,$$

推出它们的精确度依次为$14/10^2$，$13/10^4$，$8/10^5$，$3/10^7$。与它们的分母相比（依次为：1，7，106，113）精确度是很高的。事实上，这些都是圆周率π的近似值，22/7是所谓“疏率”，355/113是“密率”。

这个例子表明，即使是一个分数把它表成这种形式的“分数”也是有好处的。

例3　至今，除了试算具体数值，我们还没有方法来求解不定方程

$$x^2-11y^2=1,\quad x>0,\ y>0. \tag{14}$$

这个不定方程可化为

$$x-\sqrt{11}y=\frac{1}{x+\sqrt{11}y},\quad x>0,\ y>0.$$

$$\frac{x}{y}-\sqrt{11}=\frac{1}{y(x+\sqrt{11}y)},\quad x>0,\ y>0. \tag{15}$$

这表明不定方程(14)的解x,y所给出的分数x/y是$\sqrt{11}$一个很精确的近似值。因而，我们可以试想从式(9)所得的那些$\sqrt{11}$的近似分数中去寻找(14)的解.通过验算知，由分数199/60,3970/1197得出的

$$x=199,\ y=60;\quad x=3970,\ y=1197 \tag{16}$$

是(14)的解，其它几个都不是。当然，从式(8)继续算下去得到的近似分数中还能找出解来。

这个例子启示我们，通过研究这类新形式的"分数"，有可能找到求解形如式(14)的一类不定方程的方法。

现在我们来引进连分数的概念。

定义1 设$x_0,x_1,x_2,\cdots$是一个无穷实数列，$x_j>0$，$j\geqslant1$. 对给定的$n\geqslant0$，我们把表示式

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\ddots+\cfrac{1}{x_n}}}} \tag{17}$$

称为(**n阶**)**有限连分数**，它的值是一个实数。当$x_0,\cdots,x_n$均为整数时称为(n阶)**有限简单连分数**，它的值是一个有理分数。为书写方便，把有限连分数记作

$$\langle x_0,x_1,\cdots,x_n\rangle. \tag{18}$$

设$0\leqslant k\leqslant n$，我们把有限连分数

$$\langle x_0, x_1, \cdots, x_k \rangle \tag{19}$$

称为是有限连分数(18)的**第 k 个渐近分数**．当(18)是有限简单连分数(即 $x_0, \cdots, x_n$ 均为整数)时，把 x_k ($0 \leqslant k \leqslant n$) 称为是它的**第 k 个部分商**．当式(17)(或(18))中的 $n \to \infty$ 时，我们把相应的表示式(17)(或(18))称为**无限连分数**，即表示式

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \ddots}}}, \tag{20}$$

或简记为

$$\langle x_0, x_1, x_2, \cdots \rangle. \tag{21}$$

当 x_j ($j \geqslant 0$) 均为整数时，称(20)(或(21))为**无限简单连分数**．同样的，对任意 $k \geqslant 0$，有限连分数(19)称为是无限连分数(20)(或(21))的**第 k 个渐近分数**；当(20)(或(21))是无限简单连分数时，x_k ($k \geqslant 0$) 称为是它的**第 k 个部分商**．如果存在极限

$$\lim_{k \to \infty} \langle x_0, \cdots, x_k \rangle = \theta, \tag{22}$$

那么，就说**无限连分数**(20)(或(21))**是收敛的**，θ 称为是**无限连分数**(20)(或(21))**的值**，记作

$$\langle x_0, x_1, x_2, \cdots \rangle = \theta; \tag{23}$$

若极限(22)不存在，则说**无限连分数**(20)(或(21))**是发散的**．

本章主要讨论简单连分数的基本理论及其应用．作为本节的结束，我们来证明有限连分数的一些最基本的性质，这在以后是经常要用的．

定理1 设 $x_0, x_1, x_2, \cdots$ 是无穷实数列，$x_j > 0$，$j \geqslant 1$．那么，

(i) 对任意的整数 $n \geqslant 1$，$r \geqslant 1$ 有

$$\begin{aligned} &\langle x_0, \cdots, x_{n-1}, x_n, \cdots, x_{n+r} \rangle \\ &\quad = \langle x_0, \cdots, x_{n-1}, \langle x_n, \cdots, x_{n+r} \rangle \rangle \\ &\quad = \langle x_0, \cdots, x_{n-1}, x_n + 1/\langle x_{n+1}, \cdots, x_{n+r} \rangle \rangle. \end{aligned} \tag{24}$$

特别地有

$$\langle x_0,\cdots,x_{n-1},x_n,x_{n+1}\rangle=\langle x_0,\cdots,x_{n-1},x_n+1/x_{n+1}\rangle. \tag{25}$$

(ii) 对任意实数 $\eta>0$ 及整数 $n\geqslant 0$，

$$\langle x_0,\cdots,x_{n-1},x_n\rangle>\langle x_0,\cdots,x_{n-1},x_n+\eta\rangle,\qquad 2\nmid n. \tag{26}$$

$$\langle x_0,\cdots,x_{n-1},x_n\rangle<\langle x_0,\cdots,x_{n-1},x_n+\eta\rangle,\qquad 2\mid n. \tag{27}$$

(iii) 记

$$\alpha^{(n)}=\langle x_0,\cdots,x_n\rangle. \tag{28}$$

我们有

$$\alpha^{(n)}>\alpha^{(n+r)},\qquad 2\nmid n,\ r\geqslant 1, \tag{29}$$

$$\alpha^{(n)}<\alpha^{(n+r)},\qquad 2\mid n,\ r\geqslant 1, \tag{30}$$

$$\alpha^{(1)}>\alpha^{(3)}>\alpha^{(5)}>\cdots>\alpha^{(2s-1)}>\cdots, \tag{31}$$

$$\alpha^{(0)}<\alpha^{(2)}<\alpha^{(4)}<\cdots<\alpha^{(2t)}<\cdots, \tag{32}$$

$$\alpha^{(2s-1)}>\alpha^{(2t)},\qquad s\geqslant 1,\ t\geqslant 0. \tag{33}$$

证 式（24）和（25）直接由有限连分数的定义式（17）和记号（18）推出。对 n 用归纳法来证式（26）和式(27)，当 $n=1$ 和 $n=2$ 时，式(26)和(27)显然成立。假设当 $n=2k-1$ 和 $n=2k$ $(k\geqslant 1)$ 时式(26)和(27)都成立。当 $n=2(k+1)-1=2k+1$ 时，由式(24)知

$$\langle x_0,\cdots,x_{2k+1}\rangle=\langle x_0,x_1,\langle x_2,\cdots,x_{2k+1}\rangle\rangle.$$

由假设式(26)对 $n=2k-1$ 成立，所以

$$\langle x_2,\cdots,x_{2k},x_{2k+1}\rangle>\langle x_2,\cdots,x_{2k},x_{2k+1}+\eta\rangle.$$

由上式及 $n=2$ 时式（27）成立就推出

$$\langle x_0,x_1,\langle x_2,\cdots,x_{2k},x_{2k+1}+\eta\rangle\rangle<\langle x_0,x_1,\langle x_2,\cdots,x_{2k},x_{2k+1}\rangle\rangle,$$

由此及式（24)就推出当 $n=2(k+1)-1$时式（26）成立。当 $n=2(k+1)=2k+2$ 时，由式(24)知

$$\langle x_0,\cdots,x_{2k+2}\rangle=\langle x_0,x_1,\langle x_2,\cdots,x_{2k+2}\rangle\rangle.$$

由假设式(27)对 $n=2k$ 成立，所以

$$\langle x_2,\cdots,x_{2k+1},x_{2k+2}\rangle<\langle x_2,\cdots,x_{2k+1},x_{2k+2}+\eta\rangle.$$

由上式及 $n=2$ 时式(27)成立就推出

$$\langle x_0,x_1,\langle x_2,\cdots,x_{2k+1},x_{2k+2}\rangle\rangle$$
$$<\langle x_0,x_1,\langle x_2,\cdots,x_{2k+1},x_{2k+2}+\eta\rangle\rangle.$$

由此及式（24）就推出当 $n=2(k+1)$ 时式（27）成立。这就证明了式(26)和(27)对所有 n 都成立。

由式(24)知

$$a^{(n+r)}=\langle x_0,\cdots,x_{n-1},x_n+1/\langle x_{n+1},\cdots,x_{n+r}\rangle\rangle.$$

由此及式(26)和(27)就分别推出式（29）和(30)。取 $n=1$，$r=2,4,6,\cdots$，从式（29）就推出式(31)。取 $n=0$，$r=2,4,6,\cdots$，从式(30)就推出式(32)。最后，由式（29）及式（30）得

$$a^{(2s-1)}>a^{(2s-1+2t+1)}=a^{(2s+2t)}>a^{(2t)},$$

这就证明了式(33)。证毕①。

下面要证明的性质是：如何给出一个明确的公式，用 $x_0,x_1,\cdots,x_n$ 来表示连分数 $\langle x_0,\cdots,x_n\rangle$ 的值。先来考虑几个具体表达式。

$$\langle x_0\rangle=\frac{x_0}{1},\qquad \langle x_0,x_1\rangle=x_0+\frac{1}{x_1}=\frac{x_0x_1+1}{x_1},$$

$$\langle x_0,x_1,x_2\rangle=\langle x_0,x_1+1/x_2\rangle=\frac{x_0(x_1+1/x_2)+1}{x_1+1/x_2}$$

$$=\frac{(x_0x_1+1)x_2+x_0}{x_1x_2+1},$$

$$\langle x_0,x_1,x_2,x_3\rangle=\langle x_0,x_1,x_2+1/x_3\rangle$$

$$=\frac{(x_0x_1+1)(x_2+1/x_3)+x_0}{x_1(x_2+1/x_3)+1}$$

$$=\frac{((x_0x_1+1)x_2+x_0)x_3+(x_0x_1+1)}{(x_1x_2+1)x_3+x_1}.$$

① 事实上，(ii)和（iii）都可由以下简单结论直接看出：一个分数 a/b（a,b 是正实数），当分母 b 变大时变小，当分母 b 变小时变大。具体的证明请读者给出。

因此，如果把 $x_0, x_1, \cdots$ 看作是实变数，那么，

$$\langle x_0, \cdots, x_{n-1}, x_n\rangle = P_n/Q_n, \qquad n \geqslant 0, \tag{34}$$

其中

$$P_n = P_n(x_0, \cdots, x_n), \qquad Q_n = Q_n(x_0, \cdots, x_n) \tag{35}$$

是变数 $x_0, \cdots, x_n$ 的整系数多项式（事实上 Q_n 和 x_0 无关），且对每个变数的方次至多为一次（为什么）.故而也可这样表示：

$$\langle x_0, \cdots, x_{n-1}, x_n\rangle = \frac{K_{n-1}x_n + D_{n-1}}{H_{n-1}x_n + E_{n-1}}, \qquad n \geqslant 1, \tag{36}$$

其中

$$K_{n-1} = K_{n-1}(x_0, \cdots, x_{n-1}), \qquad H_{n-1} = H_{n-1}(x_0, \cdots, x_{n-1}),$$
$$D_{n-1} = D_{n-1}(x_0, \cdots, x_{n-1}), \qquad E_{n-1} = E_{n-1}(x_0, \cdots, x_{n-1}),$$

都是变数 $x_0, \cdots, x_{n-1}$ 的整系数多项式。在式(36)中，保持 $x_0, \cdots, x_{n-1}$ 不变。令 $x_n \to +\infty$ 时，

$$\langle x_0, \cdots, x_{n-1}, x_n\rangle \to \langle x_0, \cdots, x_{n-1}\rangle = \frac{P_{n-1}}{Q_{n-1}}.$$

$$\frac{K_{n-1}x_n + D_{n-1}}{H_{n-1}x_n + E_{n-1}} \to \frac{K_{n-1}}{H_{n-1}}.$$

令 $x_n \to 0$ 时，

$$\langle x_0, \cdots, x_{n-1}, x_n\rangle \to \langle x_0, \cdots, x_{n-2}\rangle = \frac{P_{n-2}}{Q_{n-2}},$$

$$\frac{K_{n-1}x_n + D_{n-1}}{H_{n-1}x_n + E_{n-1}} \to \frac{D_{n-1}}{E_{n-1}}.$$

以上关系式告诉我们应该有

$$K_{n-1} = P_{n-1}, \quad H_{n-1} = Q_{n-1}, \quad D_{n-1} = P_{n-2}, \quad E_{n-1} = Q_{n-2}.$$

由此及式(34),(36) 进一步推测应有递推关系式：

$$\begin{cases} P_n = x_n P_{n-1} + P_{n-2}, \\ Q_n = x_n Q_{n-1} + Q_{n-2}. \end{cases} \tag{37}$$

一结论是正确的，下面用归纳法来严格证明。

定理2 设 $x_0, x_1, x_2, \cdots$ 是无穷实数列，$x_j > 0$，$j \geqslant 1$。再设

$$P_{-2} = 0, \quad P_{-1} = 1, \quad Q_{-2} = 1, \quad Q_{-1} = 0, \tag{38}$$

以及当 $n \geqslant 0$ 时，P_n, Q_n 由递推关系式(37)给出。那么，

$$\langle x_0, \cdots, x_n \rangle = P_n / Q_n, \quad n \geqslant 0. \tag{39}$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \quad n \geqslant -1, \tag{40}$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n x_n, \quad n \geqslant 0, \tag{41}$$

以及

$$\langle x_0, \cdots, x_{n-1}, x_n \rangle - \langle x_0, \cdots, x_{n-1} \rangle = (-1)^{n+1} (Q_n Q_{n-1})^{-1}, \quad n \geqslant 1, \tag{42}$$

$$\langle x_0, \cdots, x_{n-2}, x_{n-1}, x_n \rangle - \langle x_0, \cdots, x_{n-2} \rangle = (-1)^n x_n (Q_n Q_{n-2})^{-1}, \quad n \geqslant 2. \tag{43}$$

证 当 $n = 0$ 时，$P_0 = x_0$，$Q_0 = 1$，所以式(39)成立。假设当 $n = k (\geqslant 0)$ 时式(39)成立。当 $n = k + 1$ 时，由式(25)得

$$\langle x_0, \cdots, x_{k-1}, x_k, x_{k+1} \rangle = \langle x_0, \cdots, x_{k-1}, x_k + 1/x_{k+1} \rangle,$$

由假设当 $n = k$ 时式(39)成立及式(37)，就推出

$$\begin{aligned}\langle x_0, \cdots, x_{k-1}, x_k, x_{k+1} \rangle &= \frac{(x_k + 1/x_{k+1}) P_{k-1} + P_{k-2}}{(x_k + 1/x_{k+1}) Q_{k-1} + Q_{k-2}}, \\ &= \frac{x_{k+1}(x_k P_{k-1} + P_{k-2}) + P_{k-1}}{x_{k+1}(x_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} \\ &= \frac{x_{k+1} P_k + P_{k-1}}{x_{k+1} Q_k + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}},\end{aligned}$$

即当 $n = k + 1$ 时式(39)也成立。所以，式(39)当 $n \geqslant 0$ 时都成立。

当 $n = -1$ 时，由式(38)推出式(40)成立。当 $n \geqslant 0$ 时，由式(37)可得（消去 x_n）

$$P_n Q_{n-1} - P_{n-1} Q_n = -(P_{n-1} Q_{n-2} - P_{n-2} Q_{n-1}). \tag{44}$$

反复利用上式就推出

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1} (P_{-1} Q_{-2} - P_{-2} Q_{-1}).$$

由此及式（38）就得到式（40）。注意到当 $n\geqslant0$ 时 $Q_n>0$，由式（39）及（40），就推得式（42）。

当 $n\geqslant0$ 时，由式（37）可得

$$P_nQ_{n-2}-P_{n-2}Q_n=(P_{n-1}Q_{n-2}-P_{n-2}Q_{n-1})x_n. \qquad (45)$$

由此及式（40）就证明了式(41)。注意到当 $n\geqslant0$ 时 $Q_n>0$，由式（39）及（40）就推出式(43)。证毕。

利用定理 2 很容易推出定理 1 的（iii），即式（29）—(33)成立。详细推导留给读者。当然，那里的证明更简单。

下面来举几个例子。

例 4 求有限连分数 $\langle -2,1,2/3,2,1/2,3\rangle$ 的值。

解 我们利用式(25)来计算。

$$\begin{aligned}\langle -2,1,2/3,2,1/2,3\rangle &= \langle -2,1,2/3,2,1/2+1/3\rangle\\ &= \langle -2,1,2/3,2,5/6\rangle = \langle -2,1,2/3,2+6/5\rangle\\ &= \langle -2,1,2/3,16/5\rangle = \langle -2,1,2/3+5/16\rangle\\ &= \langle -2,1,47/48\rangle = \langle -2,1+48/47\rangle\\ &= \langle -2,95/47\rangle = -2+47/95 = -143/95.\end{aligned}$$

例 5 求有限简单连分数 $\langle 1,1,1,1,1,1,1,1,1,1\rangle$ 的各个渐近分数。

解 当然，我们可以用例 1 的方法一个一个计算，但这时利用定理 2 递推地计算出 P_n, Q_n 比较方便。按公式（38），(37)可列出下表，这里 $x_n=1$，$0\leqslant n\leqslant 9$，以及 $P_{-2}=0$，$P_{-1}=1$，$Q_{-2}=1$，$Q_{-1}=0$，

$$P_n=P_{n-1}+P_{n-2},\qquad Q_n=Q_{n-1}+Q_{n-2},\qquad n\geqslant0.$$

n	0	1	2	3	4	5	6	7	8	9
x_n	1	1	1	1	1	1	1	1	1	1
P_n	1	2	3	5	8	13	21	34	55	89
Q_n	1	1	2	3	5	8	13	21	34	55

因此，各个渐近分数 P_n/Q_n 依次为：1/1，2/1，3/2，5/3，8/5，13/8，21/13，34/21，55/34，89/55。显见，P_n，Q_n 均为 Fibonacci 数列，且有 $P_n=Q_{n+1}$，$n\geqslant 0$。

习 题 一

1．计算以下有限连分数的值和各个渐近分数：

(i) $\langle 1,2,3\rangle$，　(ii) $\langle 0,1,2,3\rangle$，　(iii) $\langle 3,2,1\rangle$，

(iv) $\langle 2,1,1,4,1,1\rangle$，　(v) $\langle -4,2,1,7,8\rangle$，

(vi) $\langle -1,1/2,1/3\rangle$，　(vii) $\langle 1/2,1/4,1/8,1/16\rangle$。

2．把下面的有理数表为有限简单连分数，并求各个渐近分数：

(i) 121/21，(ii) $-19/29$，(iii) 177/292，(iv) 873/4867。

3．求有限简单连分数 $\langle 2,1,2,1,1,4,1,1,6,1,1,8\rangle$ 的各个渐近分数及其值。并与自然对数底 e 的值比较。

4．设 a,b 是正数。证明

$$a+\sqrt{a^2+b}=2a+\cfrac{b}{2a+\cfrac{b}{2a+\cfrac{b}{a+\sqrt{a^2+b}}}},$$

以及

$$a+\sqrt{a^2+b}=\langle 2a,2a/b,2a,2a/b,2a,2a/b,\ a+\sqrt{a^2+b}\rangle.$$

5．若 $\xi_0=\langle x_0,x_1,\cdots,x_n\rangle$，$x_0>0$，则 $\xi_0^{-1}=\langle 0,x_0,x_1,\cdots,x_n\rangle$。

6．设 $\{x_j\}$，$\{P_j\}$，$\{Q_j\}$ 同 §1 定理 2。证明：

(i) 当 $n\geqslant 1$ 时，$Q_n/Q_{n-1}=\langle x_n,x_{n-1},\cdots,x_1\rangle$；

(ii) 当 $x_0>0$，$n\geqslant 0$ 时，$P_n/P_{n-1}=\langle x_n,x_{n-1},\cdots,x_1,x_0\rangle$。

7．在 §1 定理 2 的条件和符号下：证明：(i) 当 $n\geqslant 1$ 时，

$$Q_{2n}\geqslant x_1(x_2+x_4+\cdots+x_{2n})+1,$$

$$Q_{2n-1}\geqslant x_1+x_3+\cdots+x_{2n-1},$$

$$Q_n<(1+x_1)(1+x_2)\cdots(1+x_n).$$

(ii) 无限连分数$\langle x_0, x_1, x_2, \cdots\rangle$收敛的充要条件是级数$\sum_{j=0}^{\infty} x_j$发散。

(iii) $\langle 1/2, 1/2, 1/2, \cdots\rangle = (\sqrt{17}+1)/4$.

(iv) $\langle 4, 1/4, 4, 1/4, \cdots\rangle = \sqrt{20}+2$。

8. 证明：

$$\langle 0, x_1, \cdots, x_n\rangle = 1/(Q_0Q_1) - 1/(Q_1Q_2) + \cdots + (-1)^{n-1}/(Q_{n-1}Q_n).$$

9. 证明：当$n \geqslant 0$时$Q_{n+1}(x_0, x_1, \cdots, x_{n+1}) = P_n(x_1, x_2, \cdots, x_{n+1})$，这里$P_n, Q_n$同§1式(35)。

10. 证明：(i) 当$n \geqslant 0$时，

$$P_n = \begin{vmatrix} x_0 & -1 & & & & 0 \\ 1 & x_1 & -1 & & & \\ & 1 & x_2 & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & & & \ddots & x_{n-1} & -1 \\ 0 & & & & 1 & x_n \end{vmatrix}.$$

(ii) 当$n \geqslant 1$时，

$$Q_n = \begin{vmatrix} x_1 & -1 & & & & 0 \\ 1 & x_2 & -1 & & & \\ & 1 & x_3 & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & & & \ddots & x_{n-1} & -1 \\ 0 & & & & 1 & x_n \end{vmatrix}.$$

11. 证明：当$n \geqslant 1$时

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix}.$$

12. 设$\alpha^{(j)}$由§1式(28)给出，P_j, Q_j由§1定理2给出。证明：当$1 \leqslant j \leqslant n$时，

$$Q_j|Q_{j-1}\alpha^{(n)} - P_{j-1}| + Q_{j-1}|Q_j\alpha^{(n)} - P_j| = 1.$$

§2 有限简单连分数

本节讨论有限简单连分数的性质及其与有理分数的关系。

设 $a_0,a_1,a_2,\cdots$ 是一个无限整数列，$a_j\geqslant 1, j\geqslant 1$。记有限简单连分数

$$\langle a_0,a_1,\cdots,a_n\rangle = r^{(n)},\qquad n\geqslant 0. \tag{1}$$

定义整数列 $\{h_n\}$ 与 $\{k_n\}$：

$$\begin{cases} h_{-2}=0,\ h_{-1}=1,\ k_{-2}=1,\ k_{-1}=0, \\ h_n=a_nh_{n-1}+h_{n-2},\ k_n=a_nk_{n-1}+k_{n-2},\ n\geqslant 0. \end{cases} \tag{2}$$

显见，$h_0=a_0$，$h_1=a_1a_0+1$，

$$1=k_0\leqslant a_1=k_1<k_2<\cdots<k_n<\cdots,\qquad k_n\to+\infty. \tag{3}$$

这里的 $\{a_j\},\{h_n\},\{k_n\}$ 就相当于 §1 定理 2 中的 $\{x_j\},\{P_n\},\{Q_n\}$ 取整数的特殊情形，作为 §1 定理 2 的特例就得到

定理1 有限简单连分数(1)的值是有理分数，

$$r^{(n)}=\langle a_0,\cdots,a_n\rangle = h_n/k_n,\ (h_n,k_n)=1,\ n\geqslant 0, \tag{4}$$

其中 h_n,k_n 由式(2)给出。此外，还有

$$h_nk_{n-1}-h_{n-1}k_n=(-1)^{n+1},\qquad n\geqslant -1, \tag{5}$$

$$h_nk_{n-2}-h_{n-2}k_n=(-1)^n a_n,\qquad n\geqslant 0, \tag{6}$$

$$r^{(n)}-r^{(n-1)}=(-1)^{n+1}(k_nk_{n-1})^{-1},\qquad n\geqslant 1, \tag{7}$$

$$r^{(n)}-r^{(n-2)}=(-1)^n a_n(k_nk_{n-2})^{-1},\qquad n\geqslant 2. \tag{8}$$

对于给定的一个不是整数的有理分数 u_0/u_1，$u_1\geqslant 2$，如何来得到它的有限简单连分数表示式呢？§1 的例 2 实际上已经给出了这种方法。利用第一章 §5的辗转相除法可得：

$$\begin{cases} u_0=b_0u_1+u_2, & 0<u_2<u_1, \\ u_1=b_1u_2+u_3, & 0<u_3<u_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ u_{s-1}=b_{s-1}u_s+u_{s+1}, & 0<u_{s+1}<u_s, \\ u_s=b_su_{s+1}. & \end{cases} \tag{9}$$

由于 u_0/u_1 不是整数，所以 $s\geqslant 1$，以及 $b_s\geqslant 2$。设

$$\xi_j=u_j/u_{j+1},\qquad 0\leqslant j\leqslant s. \tag{10}$$

由式(9)得

$$\begin{cases}\xi_j=b_j+1/\xi_{j+1}=\langle b_j,\xi_{j+1}\rangle, & 0\leqslant j\leqslant s-1,\\ \xi_s=b_s.\end{cases} \tag{11}$$

利用§1式（24)得

$$\begin{aligned}\xi_0=u_0/u_1&=\langle b_0,\xi_1\rangle=\langle b_0,\langle b_1,\xi_2\rangle\rangle\\ &=\langle b_0,b_1,\xi_2\rangle=\langle b_0,b_1,\langle b_2,\xi_3\rangle\rangle\\ &=\langle b_0,b_1,b_2,\xi_3\rangle=\cdots\\ &=\langle b_0,b_1,\cdots,b_{s-1},\xi_s\rangle\\ &=\langle b_0,b_1,\cdots,b_s\rangle,\qquad b_s>1.\end{aligned} \tag{12}$$

这就得到了 $\xi_0=u_0/u_1$ 的有限简单连分数表示式。由于 $b_s\geqslant 2$，由§1式(25）得

$$\begin{aligned}\xi_0=u_0/u_1&=\langle b_0,b_1,\cdots,(b_s-1)+1/1\rangle\\ &=\langle b_0,b_1,\cdots,b_{s-1},b_s-1,1\rangle.\end{aligned} \tag{13}$$

这样，有理分数 u_0/u_1 就有两个有限简单连分数表示式（12）与（13),(12)的最后一个部分商 $b_s\geqslant 2$，(13）的最后一个部分商为1。那么，是否还会有别的形式的表示式呢？回答是否定的。这就是下面的唯一性定理。

定理2 设 $\langle a_0,\cdots,a_n\rangle,\langle b_0,\cdots,b_s\rangle$ 是两个有限简单连分数，$a_n>1$，$b_s>1$。若

$$\langle a_0,\cdots,a_n\rangle=\langle b_0,\cdots,b_s\rangle, \tag{14}$$

则必有 $s=n$，$a_j=b_j$，$0\leqslant j\leqslant n$。

证 不妨设 $s\geqslant n$。对 n 用归纳法。当 $n=0$ 时，若 $s\geqslant 1$，则由§1式(24）得

$$\begin{aligned}a_0&=\langle b_0,b_1,\cdots,b_s\rangle=\langle b_0,\langle b_1,\cdots,b_s\rangle\rangle\\ &=b_0+1/\langle b_1,\cdots,b_s\rangle.\end{aligned}$$

由于 $b_s>1$，所以 $\langle b_1,\cdots,b_s\rangle>1$，因此上式不可能成立。这就推

出 $s=0$，$a_0=b_0$。所以结论当 $n=0$ 时成立。假设当 $n=k(\geqslant 0)$ 时结论成立。当 $n=k+1$ 时，由 §1式(24)得（注意 $s\geqslant n\geqslant 1$）

$$\langle a_0,a_1,\cdots,a_{k+1}\rangle = a_0+1/\langle a_1,\cdots,a_{k+1}\rangle,$$
$$\langle b_0,b_1,\cdots,b_s\rangle = b_0+1/\langle b_1,\cdots,b_s\rangle.$$

由 $a_{k+1}>1$及 $b_s>1$知$\langle a_1,\cdots,a_{k+1}\rangle>1$ 及$\langle b_1,\cdots,b_s\rangle>1$。因而，由条件（14）($n=k+1$)，就推出 $a_0=b_0$及

$$\langle a_1,\cdots,a_{k+1}\rangle=\langle b_1,\cdots,b_s\rangle.$$

由归纳假设知，从上式就推得 $s=k+1$及 $a_j=b_j$，$1\leqslant j\leqslant k+1$。这就证明了当 $n=k+1$时结论也成立。所以结论对一切 $n\geqslant 0$都成立。证毕。

由定理 2 及式(12)就立即推出：

定理3 任一不是整数的有理分数 u_0/u_1有且仅有式（12）及（13）给出的两种有限简单连分数表示式，其中 $b_0,\cdots,b_s$ 由式（9）给出，$s\geqslant 1,b_s>1$。

例 1 求13/5的有限简单连分数。

解 我们按式(12)来求。

$$\begin{aligned}13/5&=\langle 2+3/5\rangle=\langle 2,5/3\rangle=\langle 2,\langle 1+2/3\rangle\rangle\\&=\langle 2,\langle 1,3/2\rangle\rangle=\langle 2,1,1+1/2\rangle\\&=\langle 2,1,1,2\rangle.\end{aligned}$$

这个有限简单连分数的特点是：从左往右和从右往左的数字是一样的（参见习题二第 5 题）。13/5还可表为

$$13/5=\langle 2,1,1,1,1\rangle.$$

例 2 求 7700/2145 的有限简单连分数，及它的各个渐近分数。

解

$$\begin{aligned}7700/2145&=\langle 3+1265/2145\rangle=\langle 3,2145/1265\rangle\\&=\langle 3,1+880/1265\rangle=\langle 3,1,1265/880\rangle\\&=\langle 3,1,1+385/880\rangle=\langle 3,1,1,880/385\rangle\\&=\langle 3,1,1,2+110/385\rangle=\langle 3,1,1,2,385/110\rangle\end{aligned}$$

$$= \langle 3,1,1,2,3+55/110\rangle = \langle 3,1,1,2,3,2\rangle$$
$$= \langle 3,1,1,2,3,1,1\rangle .$$

按§2式(2) 列表来求 h_n, k_n (见表1)及渐近分数 h_n/k_n.由表1知

表 1

n	0	1	2	3	4	5
a_n	3	1	1	2	3	2
h_n	3	4	7	18	61	140
k_n	1	1	2	5	17	39

渐近分数依次为

$$3/1, 4/1, 7/2, 18/5, 61/17, 140/39 = 7700/2145.$$

这分数值化简后为140/39。虽然原来的分数不是既约的，但渐近分数一定是既约的。利用式（7）和(8)可以计算原分数与渐近分数的误差，如

$$140/39 - 61/17 = h_5/k_5 - h_4/k_4 = 1/(k_4k_5)$$
$$= 1/(17\cdot 39) = 1/663,$$
$$140/39 - 18/5 = h_5/k_5 - h_3/k_3 = -a_5/(k_3k_5)$$
$$= -2/(5\cdot 39) = -2/195.$$

其它几个误差请读者自己计算。

习　题　二

1．设 a/b 是有理分数，$\langle a_0, \cdots, a_n\rangle$ 是它的有限简单连分数，以及 $b\geqslant 1$。证明：

$$ak_{n-1} - bh_{n-1} = (-1)^{n+1}(a,b).$$

2．具体说明第 1 题给出了求最大公约数 (a,b) 及解不定方程 $ax+by=c$ 的一个新方法。用这个方法来求解以下的最大公约数和不定方程。

(i) $205x+93y=1$;

(ii) $65x-56y=-1$;

(iii) $13x+17y=5$;

(iv) $77x+63y=40$;

(v) $(314,159)$;

(vi) $(4144,7696)$.

3. 求有理分数(i) 7/11, (ii) 173/55, (iii) −43/1001, (iv) 5391/3976, (v) −873/4867的两种有限简单连分数表示式，以及它们的各个渐近分数、渐近分数与有理分数的误差。

4. 设 $r_0=\langle a_0,\cdots,a_n\rangle, s_0=\langle b_0,\cdots,b_n,b_{n+1}\rangle$是两个有限简单连分数。试求：(i) $r_0=s_0$的充要条件；(ii) $r_0<s_0$的充要条件。

5. 设有理分数 $a/b((a,b)=1, a\geqslant b\geqslant 1)$ 的有限简单连分数是$\langle a_0,a_1,\cdots,a_n\rangle$。证明：

$$\langle a_0,a_1,\cdots,a_{n-1},a_n\rangle=\langle a_n,a_{n-1},\cdots,a_1,a_0\rangle$$

的充要条件是(i) 当 $2\nmid n$ 时，$a\mid b^2+1$；(ii) 当 $2\mid n$ 时，$a\mid b^2-1$。

6. 设 a,b,c,d 是整数，$c>d>0$，$ad-bc=\pm 1$。再设实数 $\eta\geqslant 1$。若 $\xi=(a\eta+b)/(c\eta+d)$，则 $\xi=\langle a_0,\cdots,a_n,\eta\rangle$，以及$b/d=\langle a_0,\cdots,a_{n-1}\rangle$，这里$\langle a_0,\cdots,a_n\rangle$是$a/c$的有限简单连分数表示式。

7. 设 $r^{(n)}=\langle 1,2,\cdots,n+1\rangle$，它的各个渐近分数为 h_j/k_j，$j=0,1,\cdots,n$。证明：当 $n\geqslant 3$ 时，

$$h_n=nh_{n-1}+nh_{n-2}+(n-1)h_{n-3}+\cdots+3h_1+2h_0+2h_{-1}.$$

§3 无限简单连分数

本节要讨论无限简单连分数的性质及无理数如何表为无限简单连分数。

定理1 无限简单连分数$\langle a_0,a_1,a_2,\cdots\rangle$一定是收敛的，也就是说，设 $r^{(n)}=\langle a_0,\cdots,a_n\rangle$是它的第 n 个渐近分数，那么一定存

在极限

$$\lim_{n\to\infty} r^{(n)} = \theta. \tag{1}$$

此外还有

$$r^{(0)}<r^{(2)}<\cdots<r^{(2t)}<\cdots<\theta<\cdots<r^{(2s-1)}<\cdots<r^{(3)}<r^{(1)}, \tag{2}$$

以及 θ 一定是无理数。

证　由§1定理 1 的式(31),(32),(33)可知：

(i) 有理数列 $r^{(0)}, r^{(2)}, \cdots, r^{(2t)}, \cdots$ 是严格的递增数列，且有上界 $r^{(1)} = a_0 + 1/a_1$。因此，它一定有极限：

$$\lim_{t\to\infty} r^{(2t)} = \theta'$$

且满足

$$r^{(0)}<r^{(2)}<\cdots<r^{(2t)}<\cdots<\theta'. \tag{3}$$

(ii) 有理数列 $r^{(1)}, r^{(3)}, \cdots, r^{(2s-1)}, \cdots$ 是严格的递减数列，且有下界 $r^{(0)} = a_0$。因此它一定有极限：

$$\lim_{s\to\infty} r^{(2s-1)} = \theta''$$

且满足

$$\theta''<\cdots<r^{(2s-1)}<\cdots<r^{(3)}<r^{(1)}. \tag{4}$$

(iii) 由(i),(ii)及§1的式(33)推出

$$r^{(2t)}<\theta'\leqslant\theta''<r^{(2s-1)},\quad t\geqslant 0, s\geqslant 1. \tag{5}$$

因而，由式(5)及§2式(7)推出：对任意正整数 m 有

$$0\leqslant\theta''-\theta'<r^{(2m-1)}-r^{(2m)}=(k_{2m-1}k_{2m})^{-1}.$$

由此及§2式(3)就推出 $\theta''=\theta'=\theta$。这就证明了式(1)和(2)。

下面来证明 θ 是无理数。用反证法。设 $\theta = u/v$ 是有理数。由式(2)及§2式(7)可得：对任意正整数 n 有

$$0<|\theta - r^{(n)}|<|r^{(n+1)}-r^{(n)}|=(k_n k_{n+1})^{-1},$$

因而有

$$0<\left|\frac{k_n u - h_n v}{v}\right|<\frac{1}{k_{n+1}}.$$

由于 $|k_n u - h_n v|$ 一定是整数，故由上式的左半不等式知

$|k_n u-h_n v|\geqslant 1$，因而$k_{n+1}<|v|$，但这和§2式(3)矛盾。证毕。

定理2 设$\langle a_0,a_1,a_2,\cdots\rangle$是无限简单连分数，以及记

$$\theta_n=\langle a_n,a_{n+1},\cdots\rangle,\quad n\geqslant 0. \tag{6}$$

那么有

$$a_n=[\theta_n],\quad n\geqslant 0, \tag{7}$$

及

$$\langle a_0,a_1,a_2,\cdots\rangle=\langle a_0,\cdots,a_n,\theta_{n+1}\rangle,\quad n\geqslant 0, \tag{8}$$

上式右边是一个有限连分数。

证 由定理1知所有的无限简单连分数$\langle a_n,a_{n+1},\cdots\rangle(n\geqslant 0)$都是收敛的。由定理1及§1式(24)知，

$$\begin{aligned}\theta_0&=\lim_{n\to\infty}\langle a_0,a_1,\cdots,a_n\rangle\\&=\lim_{n\to\infty}\langle a_0,\langle a_1,\cdots,a_n\rangle\rangle\\&=\lim_{n\to\infty}\{a_0+1/\langle a_1,\cdots,a_n\rangle\},\\\theta_1&=\lim_{n\to\infty}\langle a_1,\cdots,a_n\rangle>a_1\geqslant 1.\end{aligned}$$

由以上两式就推出

$$\theta_0=a_0+1/\theta_1=\langle a_0,\theta_1\rangle, \tag{9}$$

$$a_0=[\theta_0].$$

同理推出对任意的$n\geqslant 0$，

$$\theta_n=a_n+1/\theta_{n+1}=\langle a_n,\theta_{n+1}\rangle, \tag{10}$$

$$a_n=[\theta_n].$$

这就证明了式(7)。利用归纳法，由式(9)和(10)就可推出式(8)成立(留给读者)。证毕。

由式(7)立即得到

推论3 设$\langle a_0,a_1,\cdots\rangle$，$\langle b_0,b_1,\cdots\rangle$是两个无限简单连分数。若

$$\langle a_0,a_1,\cdots\rangle=\langle b_0,b_1,\cdots\rangle,$$

则$a_j=b_j$，$j\geqslant 0$。

这表明一个无理数如果能用无限简单连分数来表示(即其值

等于这个无理数)，那么这个表示式一定是唯一的。那么，任意一个无理数是否一定能用无限简单连分数来表示呢？回答是肯定的。事实上，§1 例 1 和定理 2 已经指出了具体求这种表示式的方法，但需要严格证明。

定理4 设 ξ_0 是一个无理数。再设

$$\begin{cases} a_0=[\xi_0], & \xi_1=1/\{\xi_0\}, \\ a_j=[\xi_j], & \xi_{j+1}=1/\{\xi_j\},\ j\geqslant 1. \end{cases} \tag{11}$$

那么，有 $a_j\geqslant 1, j\geqslant 1$，及

$$\xi_0=\langle a_0,a_1,a_2,\cdots\rangle. \tag{12}$$

我们把$\langle a_0,a_1,a_2,\cdots\rangle$称为是**无理数 ξ_0 的无限简单连分数表示式。**

证 由于 ξ_0 是无理数，所以 $\xi_j(j\geqslant 1)$都是无理数。因此，$0<\{\xi_j\}<1, j\geqslant 0$，以及 $\xi_j>1, a_j\geqslant 1, j\geqslant 1$。由定理 1 知式(12)右边的无限简单连分数是收敛的，设

$$\theta_0=\langle a_0,a_1,a_2,\cdots\rangle.$$

我们要来证明 $\theta_0=\xi_0$。由 $x=[x]+\{x\}$及式(11)可得

$$\begin{aligned}\xi_0&=a_0+1/\xi_1=\langle a_0,\xi_1\rangle=\langle a_0,a_1+1/\xi_2\rangle=\langle a_0,a_1,\xi_2\rangle\\ &=\cdots=\langle a_0,a_1,\cdots,a_n,\xi_{n+1}\rangle,\quad n\geqslant 0.\end{aligned} \tag{13}$$

由此及 §1定理 1 得

$$r^{(0)}<r^{(2)}<\cdots<r^{(2s)}<\cdots<\xi_0<\cdots<r^{(2s-1)}<\cdots<r^{(3)}<r^{(1)}, \tag{14}$$

这里

$$r^{(n)}=\langle a_0,a_1,\cdots,a_n\rangle,\quad n\geqslant 0.$$

由此及式(1)就推出 $\theta_0=\xi_0$。证毕。

由定理 4 立即得到 ξ_n 的无限简单连分数表示式：

$$\xi_n=\langle a_n,a_{n+1},\cdots\rangle,\quad n\geqslant 0. \tag{15}$$

我们把 ξ_n 称为 ξ_0 的**第 n 个完全商。**

例 1 求$\langle 1,1,1,1,\cdots\rangle$的值。

解 设值为 θ。由式(8)知

$$\theta=\langle 1,\theta\rangle=1+1/\theta.$$

因此，$\theta^2-\theta-1=0$，所以

$$\theta=(1\pm\sqrt{5})/2.$$

由此及 $\theta>1$ 知，$\theta=(1+\sqrt{5})/2$。

例 2 求 $\langle -1,3,1,2,4,1,2,4,1,2,4,\cdots\rangle$ 的值 θ。

解 先求 $\langle 1,2,4,1,2,4,1,2,4,\cdots\rangle$ 的值，设为 θ'。由式(8)知(利用§1式(25))

$$\begin{aligned}\theta'&=\langle 1,2,4,\theta'\rangle=\langle 1,2,4+1/\theta'\rangle\\&=\langle 1,2,(4\theta'+1)/\theta'\rangle=\langle 1,2+\theta'/(4\theta'+1)\rangle\\&=\langle 1,(9\theta'+2)/(4\theta'+1)\rangle=1+(4\theta'+1)/(9\theta'+2)\\&=(13\theta'+3)/(9\theta'+2).\end{aligned}$$

因此，$9(\theta')^2-11\theta'-3=0$，

$$\theta'=(11\pm\sqrt{229})/18.$$

由此及 $\theta'>1$ 知 $\theta'=(11+\sqrt{229})/18$。因而，由式(8)知

$$\begin{aligned}\theta&=\langle -1,3,\theta'\rangle=\langle -1,3,(11+\sqrt{229})/18\rangle\\&=\langle -1,3+18/(11+\sqrt{229})\rangle\\&=\langle -1,3+(\sqrt{229}-11)/6\rangle\\&=\langle -1,(\sqrt{229}+7)/6\rangle\\&=-1+6/(\sqrt{229}+7)\\&=(\sqrt{229}-37)/6.\end{aligned}$$

例 3 求例 2 中的连分数的各个完全商。

解 我们只要求 $\xi_0=\theta,\xi_1=\langle 3,\theta'\rangle,\xi_2=\theta',\xi_3=\langle 2,4,\theta'\rangle,\xi_4=\langle 4,\theta'\rangle$。因为当 $n\geqslant 5$ 时，$\xi_n=\xi_{n-3}$。这样，只要求

$$\xi_1=\langle 3,\theta'\rangle=3+18/(11+\sqrt{229})=(\sqrt{229}+7)/6.$$

$$\xi_4=\langle 4,\theta'\rangle=4+18/(11+\sqrt{229})=(\sqrt{229}+13)/6.$$

$$\begin{aligned}\xi_3&=\langle 2,4,\theta'\rangle=\langle 2,\langle 4,\theta'\rangle\rangle=\langle 2,\xi_4\rangle\\&=2+6/(\sqrt{229}+13)=(\sqrt{229}+7)/10.\end{aligned}$$

例 4 求 $\sqrt{8}$ 的无限简单连分数。

解 按式(13)可得

$$\begin{aligned}\sqrt{8}&=2+(\sqrt{8}-2)=2+4/(\sqrt{8}+2)\\&=\langle 2,(\sqrt{8}+2)/4\rangle\\&=\langle 2,1+(\sqrt{8}-2)/4\rangle=\langle 2,1,\sqrt{8}+2\rangle\\&=\langle 2,1,4+(\sqrt{8}-2)\rangle\\&=\langle 2,1,4,(\sqrt{8}+2)/4\rangle,\end{aligned}$$

这又回到$\langle 2,(\sqrt{8}+2)/4\rangle$的情形，因此，数字循环出现，得到

$$\sqrt{8}=\langle 2,1,4,1,4,1,4,\cdots\rangle.$$

我们同时得到了

$$(\sqrt{8}+2)/4=\langle 1,4,1,4,1,4,\cdots\rangle,$$

$$\sqrt{8}+2=\langle 4,1,4,1,4,1,\cdots\rangle.$$

例 4 的方法可用于来求形如$(\sqrt{d}+a)/b$的无限简单连分数，这将在§5作进一步讨论，但求一般无理数的无限简单连分数是十分困难的。下面来举个例子。

例 5 求$\sqrt[3]{2}$的无限简单连分数的前六个数字。

解 由定理 4 知，设$\xi_0=\sqrt[3]{2}$。

$$a_0=[\xi_0]=1,\quad \xi_1=(\xi_0-a_0)^{-1}=(\sqrt[3]{2}-1)^{-1}$$
$$=\sqrt[3]{4}+\sqrt[3]{2}+1,$$

$$a_1=[\xi_1]=3,\quad \xi_2=(\xi_1-3)^{-1}=(\sqrt[3]{4}+\sqrt[3]{2}-2)^{-1}$$
$$=\frac{\sqrt[3]{4}+\sqrt[3]{2}+1}{\sqrt[3]{2}+2},$$

$$a_2=[\xi_2]=1,\quad \xi_3=(\xi_2-1)^{-1}=\frac{\sqrt[3]{2}+2}{\sqrt[3]{4}-1}$$
$$=\frac{4\sqrt[3]{4}+5\sqrt[3]{2}+4}{3},$$

$$a_3=[\xi_3]=5,\quad \xi_4=(\xi_3-5)^{-1}=\frac{3}{4\sqrt[3]{4}+5\sqrt[3]{2}-11},$$

$$a_4=[\xi_4]=1,\quad \xi_5=(\xi_4-1)^{-1}=\frac{4\sqrt[3]{4}+5\sqrt[3]{2}-11}{14-5\sqrt[3]{2}-4\sqrt[3]{4}},$$

$$a_5=[\xi_5]=1,\quad \xi_6=(\xi_5-1)^{-1}=\frac{14-5\sqrt[3]{2}-4\sqrt[3]{4}}{8\sqrt[3]{4}+10\sqrt[3]{2}-25}.$$

所以，

$$\sqrt[3]{2}=\langle 1,3,1,5,1,1,\xi_6\rangle.$$

实际上利用计算器求 a_n 时，不用求出 ξ_n 的精确表示式，当然不能求太多位数字，以免误差太大，使 a_n 的值失真。但这里是可以的。

$$\begin{aligned}
&\xi_0=\sqrt[3]{2}\approx 1.25992105,\quad a_0=1,\\
&\xi_1=(\xi_0-1)^{-1}\approx 3.847322102,\quad a_1=3,\\
&\xi_2=(\xi_1-3)^{-1}\approx 1.180188736,\quad a_2=1,\\
&\xi_3=(\xi_2-1)^{-1}\approx 5.549736484,\quad a_3=5,\\
&\xi_4=(\xi_3-5)^{-1}\approx 1.819053362,\quad a_4=1,\\
&\xi_5=(\xi_4-1)^{-1}\approx 1.220921671,\quad a_5=1,\\
&\xi_6=(\xi_5-1)^{-1}\approx 4.526491197.
\end{aligned}$$

下面来讨论无理数用它的无限简单连分数的渐近分数来作有理逼近时的误差，并证明这种有理逼近是最佳的。

设无理数 ξ_0 的无限简单连分数表示式由式(12)给出，它的第 n 个渐近分数是

$$r^{(n)}=\langle a_0,a_1,\cdots,a_n\rangle,$$

以及整数列 $\{h_n\}$，$\{k_n\}$ 由 §2式(2)给出。我们先来证明：

定理5 对 $n\geqslant 0$ 有

$$\frac{1}{k_n(k_n+k_{n+1})}<|\xi_0-r^{(n)}|=\left|\xi_0-\frac{h_n}{k_n}\right|<\frac{1}{k_nk_{n+1}}.\qquad(16)$$

证 由式(13)及§1定理2的式(39)得到

$$\xi_0 = \langle a_0, \cdots, a_n, \xi_{n+1} \rangle$$

$$= \frac{h_n \xi_{n+1} + h_{n-1}}{k_n \xi_{n+1} + k_{n-1}}, \quad n \geqslant 0. \tag{17}$$

由此及§2定理1得

$$\xi_0 - r^{(n)} = \xi_0 - \frac{h_n}{k_n} = \frac{k_n h_{n-1} - k_{n-1} h_n}{k_n (k_n \xi_{n+1} + k_{n-1})}$$

$$= \frac{(-1)^n}{k_n (k_n \xi_{n+1} + k_{n-1})}, \quad n \geqslant 0. \tag{18}$$

由于 $a_{n+1} < \xi_{n+1} < a_{n+1} + 1$，利用§2式(2)得：$n \geqslant 0$ 时，

$$k_{n+1} = a_{n+1} k_n + k_{n-1} < k_n \xi_{n+1} + k_{n-1}$$

$$< a_{n+1} k_n + k_{n-1} + k_n = k_{n+1} + k_n. \tag{19}$$

由以上两式即得式(16)。证毕。

由§2的式(2)知，

$$k_n + k_{n+1} \leqslant k_{n+2}.$$

由此及式(16)得：当 $n \geqslant 0$ 时，

$$\left| \xi_0 - \frac{h_{n+1}}{k_{n+1}} \right| < \frac{1}{k_{n+1} k_{n+2}} \leqslant \frac{1}{k_n (k_n + k_{n+1})} < \left| \xi_0 - \frac{h_n}{k_n} \right|, \tag{20}$$

及

$$|k_{n+1} \xi_0 - h_{n+1}| < \frac{1}{k_{n+2}} \leqslant \frac{1}{k_n + k_{n+1}} < |k_n \xi_0 - h_n|. \tag{21}$$

以上给出了用渐近分数去逼近无限简单连分数时的误差估计。式(20)与(21)表明渐近分数依次一个比一个更接近 ξ_0。下面来指出无理数的这种有理逼近在某种意义上说是最佳的。

定理5 设有理分数 a/b 具有正的分母 b。那么，

(i) 若对某个 $n \geqslant 0$ 有

$$|\xi_0 b - a| < |\xi_0 k_n - h_n|, \tag{22}$$

则 $b\geqslant k_{n+1}$。

（ii）若对某个 $n\geqslant 1$ 有

$$|\xi_0-a/b|<|\xi_0-h_n/k_n|,\tag{23}$$

则 $b>k_n$。

证 证明的关键在于要把 a/b 和渐近分数建立联系。由§2式(5)知 $k_nh_{n+1}-k_{n+1}h_n=(-1)^n$，所以线性方程组

$$\begin{cases} xk_n+yk_{n+1}=b, \\ xh_n+yh_{n+1}=a \end{cases}$$

有整数解

$$x=(-1)^n(bh_{n+1}-ak_{n+1}),\quad y=(-1)^n(-bh_n+ak_n).$$

这样就有整数 x,y 使得

$$\xi_0b-a=x(\xi_0k_n-h_n)+y(\xi_0k_{n+1}-h_{n+1}).\tag{24}$$

我们用反证法来证(i)。若 $0<b<k_{n+1}$，我们来证这时必有

$$xy<0.\tag{25}$$

因为，如果 $x=0$，则 $b=yk_{n+1}\geqslant k_{n+1}$（注意 $b>0$），这和假设 $0<b<k_{n+1}$ 矛盾；如果 $y=0$，则 $b=xk_n,a=xh_n$，因而有 $|\xi_0b-a|=x|\xi_0k_n-h_n|$，这和条件(22)矛盾。这就证明了 $xy\neq 0$。如果 $xy>0$，则有 $b=|x|k_n+|y|k_{n+1}>k_{n+1}$ 这又和假设 $0<b<k_{n+1}$ 矛盾。所以，若 $0<b<k_{n+1}$，则必有式(25)成立。

但另一方面，由式(14)知 $\xi_0k_n-h_n$ 依次交替改变正负号（这由式(18)也可看出）。因此，当式(25)成立时，由式(24)推出

$$\begin{aligned}|\xi_0b-a|&=|x||\xi_0k_n-h_n|+|y||\xi_0k_{n+1}-h_{n+1}|\\ &>|\xi_0k_n-h_n|.\end{aligned}$$

这和条件(22)矛盾。这就证明了(i)。

由(i)立即可推出(ii)。条件(23)可改写为

$$|\xi_0b-a|<(b/k_n)|\xi_0k_n-h_n|,\quad n\geqslant 1.\tag{26}$$

若 $b\leqslant k_n$，则条件(26)推出条件(22)成立，因而由已证明的(i)推出 $b\geqslant k_{n+1}$。但当 $n\geqslant 1$ 时，由§2式(3)知 $k_{n+1}>k_n$，矛盾。所以当 $n\geqslant 1$ 时必有 $b>k_n$。证毕。

下面的定理表明：一个无理数的"好的"有理分数逼近一定是它的渐近分数①给出的逼近。

定理7 设ξ_0是无理数。若有有理分数$a/b, b\geqslant 1$，使得

$$|\xi_0-a/b|<1/(2b^2), \tag{27}$$

那么，a/b一定是ξ_0的某个渐近分数。

证 由§2式(3)知，存在唯一的n使得

$$k_n\leqslant b<k_{n+1}. \tag{28}$$

先来证明必有$b=k_n$。若不然，必有

$$k_n<b<k_{n+1}, \tag{29}$$

及a/b不是渐近分数(为什么)。因而有

$$|h_n/k_n-a/b|\geqslant 1/(bk_n). \tag{30}$$

由$b<k_{n+1}$从定理6(i)推出

$$|\xi_0 k_n-h_n|\leqslant|\xi_0 b-a|, \tag{31}$$

这样，由式(30)，(31)及条件(27)得到

$$1/(bk_n)\leqslant|h_n/k_n-a/b|\leqslant|\xi_0-h_n/k_n|+|\xi_0-a/b|$$
$$<1/(2bk_n)+1/(2b^2).$$

由上式推出$b<k_n$，矛盾。所以，必有$b=k_n$。进而由上式的右半不等式(这是由条件(27)及式(31)推出的，所以一定成立)得到

$$|h_n/k_n-a/k_n|<1/k_n^2,$$

即$|h_n-a|<1/k_n$，所以，$a=h_n$。因此，$a/b=h_n/k_n$是ξ_0的一个渐近分数。证毕。

定理7并未回答像式(27)这样"好的"逼近是否一定存在，也就是说利用无理数的渐近分数去逼近它时是否一定有这样"好的"逼近存在。回答是肯定的，这将在下节作进一步讨论。

作为定理7的一个应用，我们来部分地回答§1例3提出的问题。

定理8 设$d>1$不是平方数。若不定方程

① 一个无理数的渐近分数就是指它的无限简单连分数表示式的渐近分数。

$$x^2 - dy^2 = \pm 1 \tag{32}$$

有解 $x = x_0 > 0, y = y_0 > 0$。那么，x_0/y_0 一定是 $\sqrt{d}$ 的某个渐近分数 h_n/k_n，且 $x_0 = h_n, y_0 = k_n$。

证 这时必有 $x_0 \geqslant y_0$。若不然，从 $y_0 > x_0$ 可推出

$$\pm 1 = x_0^2 - dy_0^2 < y_0^2 - dy_0^2 \leqslant -y_0^2 \leqslant -1.$$

这不可能。由 x_0, y_0 是解及 $x_0 \geqslant y_0$ 可得

$$|x_0/y_0 - \sqrt{d}| = 1/(y_0^2(x_0/y_0 + \sqrt{d})) < 1/(2y_0^2).$$

$\sqrt{d}$ 是无理数（为什么），利用上式，由定理 7 就推出 x_0/y_0 必为 $\sqrt{d}$ 的渐近分数 h_n/k_n，由此及 $(x_0, y_0) = 1$ 即得 $x_0 = h_n, y_0 = k_n$。证毕。

虽然，定理 8 并未回答不定方程(32)是否有解，但结论表明，我们只要在 $\sqrt{d}$ 的渐近分数中去寻找(32)的解。这就要求我们去研究 $\sqrt{d}$ 的无限简单连分数表示式的性质，这将在 § 5 讨论。

例 6 求 $\sqrt{8}$ 的分母最小的渐近分数，其误差 $\leqslant 10^{-6}$。

在例 4 中已求出 $\sqrt{8} = \langle 2,1,4,1,4,1,4,\cdots \rangle$。我们先列表求出 h_n, k_n，然后根据式(16)估计误差。

n	0	1	2	3	4	5	6	7	8	9
a_n	2	1	4	1	4	1	4	1	4	1
h_n	2	3	14	17	82	99	478	577	2786	3363
k_n	1	1	5	6	29	35	169	204	985	1189

由上表知，取 $n = 8, 7$ 时，由式(16)可得

$$\left|\sqrt{8} - \frac{h_8}{k_8}\right| = \left|\sqrt{8} - \frac{2786}{985}\right| < \frac{1}{985 \cdot 1189}$$

$$= \frac{1}{1171165} < 10^{-6},$$

$$\left|\sqrt{8}-\frac{h_7}{k_7}\right|=\left|\sqrt{8}-\frac{577}{204}\right|>\frac{1}{204(204+985)}$$

$$=\frac{1}{242556}>10^{-6}。$$

因此要求的渐近分数是 $h_8/k_8=2786/985$。

习 题 三

1．求以下无限简单连分数的值：

(i) $\langle 2,3,1,1,1,\cdots\rangle$；

(ii) $\langle 1,2,3,1,2,3,1,2,3,\cdots\rangle$；

(iii) $\langle 0,2,1,3,1,3,1,3,\cdots\rangle$；

(iv) $\langle -2,2,1,2,1,2,1,\cdots\rangle$。

2．设 a，b 是正整数，a 整除 b，即$b=ac$。证明：

$$\langle b,a,b,a,b,a,\cdots\rangle=(b+\sqrt{b^2+4c})/2。$$

3．求以下无理数的无限简单连分数，前六个渐近分数，前七个完全商，以及该无理数和它的前六个渐近分数的差。

(i) $\sqrt{7}$，(ii) $\sqrt{13}$，(iii) $\sqrt{29}$，(iv) $(\sqrt{10}+1)/3$，

(v) $(5-\sqrt{37})/3$。

4．设 α,β 是无理数，它们的无限简单连分数是：

$$\alpha=\langle a_0,a_1,a_2,\cdots\rangle,\qquad \beta=\langle b_0,b_1,b_2,\cdots\rangle。$$

证明：$\alpha>\beta$ 的充要条件是存在唯一 $n\geqslant 0$ 使得：(i) 当 $2|n$ 时，$a_j=b_j\,(0\leqslant j<n)$，$a_n>b_n$；(ii) 当$2\nmid n$时，$a_j=b_j\,(0\leqslant j<n)$，$a_n<b_n$。

5．设 ξ_0是无理数，它的无限简单连分数是$\langle a_0,a_1,a_2,\cdots\rangle$.证明：当 $a_1>1$ 时，$-\xi_0=\langle -a_0-1,1,a_1-1,a_2,a_3,\cdots\rangle$；当 $a_1=1$ 时，$-\xi_0=\langle -a_0-1,a_2+1,a_3,\cdots\rangle$。

6．我们说数 β 等价于数α，如果存在整数 a,b,c,d，满足 $ad-bc=\pm 1$，使得$\beta=(a\alpha+b)/(c\alpha+d)$。证明：(i) 任意的数 α必与

自身等价。(ii) 若β等价于α，则α等价于β。(iii) 若α等价于β，β等价于γ，则α等价于γ。(iv) 有理数一定等价于零。(v) 任意两个有理数一定等价。(vi) 设α,β是两个实无理数。那么，α与β等价的充要条件是它们的无限简单连分数为如下形式：

$$\alpha=\langle a_0,\cdots,a_m,c_0,c_1,c_2,\cdots\rangle,$$
$$\beta=\langle b_0,\cdots,b_n,c_0,c_1,c_2,\cdots\rangle.$$

7. 证明：当$k_1>1$时，定理 6 (ii)对$n=0$也成立。

8. 举例说明定理 6 (ii)中的 $b>k_n$ 不能改进为 $b\geqslant k_{n+1}$(取$\sqrt{2}$及它的渐近分数 h_3/k_3，即$n=3$)。

9. 设ξ_0是实数，a,b是整数，$b\geqslant 1$。证明：有

$$|b\xi_0-a|=\min_{0<y<b}|y\xi_0-x| \qquad (*)$$

成立的充要条件是a/b是ξ_0的渐近分数，这里y取整数，x取任意整数。

10. 设ξ_0为无理数，它的无限简单连分数是$\langle a_0,a_1,a_2,\cdots\rangle$，$h_n/k_n$是它的渐近分数。对取定的$n\geqslant 1$，考虑数组：$(h_{n-1}+lh_n)/(k_{n-1}+lk_n)$，$0\leqslant l\leqslant a_{n+1}$。证明：当$n$是奇数时，这数组递增；当$n$是偶数时递减。我们把所有分数$(h_{n-1}+lh_n)/(k_{n-1}+lk_n)$，$0<l<a_{n+1}$，$n\geqslant 1$，称为是$\xi_0$的第二渐近分数。

11. 设ξ_0是实数，a,b是整数，$b\geqslant 1$。证明若有

$$|\xi_0-a/b|=\min_{0<y<b}|\xi_0-x/y|, \qquad (**)$$

则a/b一定是ξ_0的渐近分数或第二渐近分数，这里x和y的取值同第 9 题。举例说明，对于第二渐近分数不一定有式(**)成立。

12. 证明：若第 9 题中的式(*)成立则必有第11题中的(**)成立。

13. 设ξ_0是无理数，它的无限简单连分数是$\langle a_0,a_1,a_2,\cdots\rangle$。再设$b_1,b_2,b_3,\cdots$是一有限或无限正整数列，以及$\eta_n=\langle a_0,\cdots,a_n,$

$b_1, b_2, b_3, \cdots\rangle$。证明：$\lim\limits_{n\to\infty}\eta_n=\xi_0$。

§4 无理数的最佳可能有理逼近

设ξ_0是无理数，$h_n/k_n(n\geqslant 0)$是ξ_0的渐近分数。由§2式(3)及§3式(16)知，对每个渐近分数h_n/k_n有

$$|\xi_0-h_n/k_n|<1/k_n^2,\qquad n\geqslant 0. \tag{1}$$

§3定理7证明了：若用有理分数a/b去逼近ξ_0时有误差估计式§3(27)成立，那么，a/b一定是ξ_0的渐近分数。下面的定理将指出这样的渐近分数不仅一定存在，而且是很多的。

定理1 设$n\geqslant 0$，h_n/k_n，h_{n+1}/k_{n+1}是无理数ξ_0的两个相邻的渐近分数。那么，

$$|\xi_0-h_n/k_n|<1/(2k_n^2),$$

或

$$|\xi_0-h_{n+1}/k_{n+1}|<1/(2k_{n+1}^2),$$

至少有一个成立。

证 若两式都不成立，那么利用§3式(14)可得

$$\begin{aligned}1/(2k_n^2)+1/(2k_{n+1}^2)&\leqslant|\xi_0-h_n/k_n|+|\xi_0-h_{n+1}/k_{n+1}|\\&\leqslant|h_n/k_n-h_{n+1}/k_{n+1}|=1/(k_nk_{n+1}),\end{aligned}$$

最后一步用到了§2式(5)。进而有

$$2k_nk_{n+1}\geqslant k_n^2+k_{n+1}^2.$$

而这仅当$k_n=k_{n+1}$时才能成立。由此及§2式(3)知，必有$n=0$，$k_0=k_1=a_1=1$，$h_0=a_0$，$h_1=a_1a_0+1$。故有

$$a_0+1/2<\xi_0<a_0+1,\qquad h_1/k_1=a_0+1.$$

由此推出

$$|\xi_0-h_1/k_1|=|\xi_0-(a_0+1)|<1/2=1/(2k_1^2).$$

这和假设矛盾。证毕。

由定理1立即推出：

推论2 当$\lambda=2$时，存在无穷多个有理分数a/b满足

$$|\xi_0-a/b|<1/(\lambda b^2)。\tag{2}$$

立即会提出的一个问题是推论 2 中的 λ 的取值能否进一步改进。在一般情形下，下面的定理完全回答了这一问题。

定理3 设ξ_0是无理数，h_{n-1}/k_{n-1}，h_n/k_n，h_{n+1}/k_{n+1} $(n\geqslant1)$是ξ_0的三个相邻的渐近分数。那么，以下三个不等式

$$|\xi_0-h_j/k_j|<1/(\sqrt{5}k_j^2),\qquad j=n-1,n,n+1$$

至少有一个成立。

为此先证明一个引理。

引理4 设实数 $x\geqslant1$及 $x+x^{-1}<\sqrt{5}$。那么，必有$1\leqslant x<(\sqrt{5}+1)/2$。

证 当$x\geqslant1$时，函数$x+x^{-1}$是x的增函数。因为，当$x_1\geqslant1$，$x_2\geqslant1$，$x_1\neq x_2$时

$$x_1+x_1^{-1}>x_2+x_2^{-1}$$

等价于

$$(x_1x_2-1)(x_1-x_2)>0。$$

由于$x_1x_2>1$，所以等价于$x_1>x_2$。这就证明了所要结论。使$x+x^{-1}=\sqrt{5}$成立的$x=(\sqrt{5}\pm1)/2$，由此及$x+x^{-1}$当$x\geqslant1$时是增函数就推出引理的结论。

定理3的证明 用反证法。设$q_j=k_j/k_{j-1}$，$j=n,n+1$。假设三个不等式都不成立。由假设及§3式(15)，§2式(5)可得

$$\frac{1}{k_jk_{j-1}}=\left|\frac{h_j}{k_j}-\frac{h_{j-1}}{k_{j-1}}\right|=\left|\frac{h_j}{k_j}-\xi_0\right|+\left|\xi_0-\frac{h_{j-1}}{k_{j-1}}\right|$$

$$\geqslant\frac{1}{\sqrt{5}k_j^2}+\frac{1}{\sqrt{5}k_{j-1}^2},\qquad j=n,n+1。$$

由此推出

$$q_j+q_j^{-1}\leqslant\sqrt{5},\qquad j=n,n+1。$$

由$\sqrt{5}$是无理数知上式中的等号不能成立，此外，由§2式(3)知

$q_n \geqslant 1$，$q_{n+1} \geqslant 1$。因而由引理 4 得

$$1 \leqslant q_j < (\sqrt{5}+1)/2, \quad j = n, n+1. \tag{3}$$

但另一方面，由 § 2式(3)知

$$q_{n+1} = (a_{n+1}k_n + k_{n-1})/k_n = a_{n+1} + q_n^{-1} \geqslant 1 + q_n^{-1}.$$

由此及$q_n < (\sqrt{5}+1)/2$，可推出$q_{n+1} > (\sqrt{5}+1)/2$，这和式(3)($j = n+1$)矛盾。证毕。

由定理 3 立即推出：

推论5 当取$\lambda = \sqrt{5}$时，存在无穷多个有理分数 a/b 满足式(2)。

$\lambda = \sqrt{5}$这一数值能否进一步改进呢？一般说来是不可能的。§ 3的式(18)及(16)刻画了用渐近分数去逼近无理数ξ_0时的误差。由 § 3式(18)可得

$$|\xi_0 - h_n/k_n| = \frac{1}{k_n^2(\xi_{n+1} + k_{n-1}/k_n)}, \quad n \geqslant 0. \tag{4}$$

所以，对一个取定的无理数ξ_0来说，只要取

$$\lambda < \lambda(\xi_0) = \overline{\lim_{n\to\infty}}(\xi_{n+1} + k_{n-1}/k_n), \tag{5}$$

就会有无穷多个渐近分数取作 a/b 时使式(2)成立；而当取$\lambda > \lambda(\xi_0)$时，一定不可能有无穷多个有理分数 a/b 使式(2)成立；而取$\lambda = \lambda(\xi_0)$时要看具体情形而定。这样，推论 5 表明，对所有的无理数ξ_0有

$$\lambda(\xi_0) \geqslant \sqrt{5}. \tag{6}$$

因而为了证明推论 5 中的$\sqrt{5}$是不能改进的，就只要去找一个无理数η_0，使得

$$\lambda(\eta_0) = \sqrt{5}. \tag{7}$$

如何去找η_0呢？从式(4)和 § 3(16)大致可看出，这一η_0对应的 k_n 应尽量的小，而由 § 2式(2)知，这就是对应的a_n应尽量的小。由于$a_n \geqslant 1 (n \geqslant 1)$，我们来考虑无理数

$$\eta_0 = \langle 1, 1, 1, \cdots \rangle. \tag{8}$$

由§3式(8)知

$$\eta_0 = \langle 1, \eta_0 \rangle = 1 + \eta_0^{-1},$$

所以

$$\eta_0 = (\sqrt{5} + 1)/2. \tag{9}$$

显见，$\eta_n = \eta_0 = (\sqrt{5} + 1)/2$，$n \geqslant 0$。由§2式(2)知，这里

$$h_0 = k_1 = 1, \quad h_1 = k_2 = 2,$$

$$h_n = h_{n-1} + h_{n-2}, \quad k_n = k_{n-1} + k_{n-2}.$$

因而得(用归纳法证)

$$k_{n+1} = h_n, \quad n \geqslant 0.$$

所以有

$$\lambda(\eta_0) = \lim_{n \to \infty} \left(\eta_{n+1} + \frac{k_{n-1}}{k_n} \right)$$

$$= \lim_{n \to \infty} \left(\eta_{n+1} + \frac{k_{n-1}}{h_{n-1}} \right)$$

$$= \eta_0 + \eta_0^{-1} = \sqrt{5}.$$

这就证明了：

定理6 当$\xi_0 = (\sqrt{5} + 1)/2$时，对任意取定的$\lambda > \sqrt{5}$，不可能有无穷多个有理分数a/b使式(2)成立。因而，推论5中的常数$\sqrt{5}$是最优的。

以上我们利用无理数的无限简单连分数表示式的渐近分数来讨论了无理数的有理逼近问题。这一问题还可用 Farey 分数作为工具来讨论，这些将安排在习题中，最后我们来指出，利用鸽巢原理可以很容易证明形如式(1)的有理逼近定理。

定理7 设α是一实数。那么，对任给的正数$x \geqslant 1$，一定存在整数a, b，满足

$$1 \leqslant b \leqslant x, \quad (a, b) = 1, \tag{10}$$

使得

$$|\alpha - a/b| < 1/(bx). \tag{11}$$

证　显见，以下$[x]+2$个数

$$1, \quad j\alpha-[j\alpha], \quad j=0,1,\cdots,[x],$$

均位于区间$[0,1]$上，因而由鸽巢原理知必有两个数，其差不超过$([x]+1)^{-1}$。如果这两个数是

$$j_1\alpha-[j_1\alpha], \quad j_2\alpha-[j_2\alpha], \quad 0\leqslant j_1<j_2\leqslant[x],$$

那么，我们就取$d=j_2-j_1$，$c=[j_2\alpha]-[j_1\alpha]$，及

$$a=c/(c,d), \quad b=d/(c,d).$$

不然，这两个数一定是

$$1, \quad j_1\alpha-[j_1\alpha], \quad 0\leqslant j_1\leqslant[x],$$

这时就取$d=j_1$，$c=[j_1\alpha]+1$，及

$$a=c/(c,d), \quad b=d/(c,d).$$

容易验证，无论何种情形，对所取的a,b均满足式(10)，且

$$|\alpha-a/b|\leqslant 1/(b([x]+1)), \tag{12}$$

由此即推出式(11)成立。证毕。

由定理7立即推出：

定理8　设ξ_0是一无理数。那么，一定存在无穷多个有理分数a/b使得

$$|\xi_0-a/b|<1/b^2 \tag{13}$$

成立。

证　在定理7中取$\alpha=\xi_0$，对$x_0=1$，一定存在整数a_0使

$$0<y_0=|\xi_0-a_0/1|<1,$$

由于ξ_0是无理数，所以$y_0>0$，仍由定理7推出：对$x_1=y_0^{-1}$，必有

$$1\leqslant b_1<x_1, \quad (a_1,b_1)=1,$$

使得(因ξ_0为无理数)

$$0<y_1=|\xi_0-a_1/b_1|<1/(b_1x_1)<1/b_1^2.$$

一般地，如果已经求出a_n,b_n满足

$$1\leqslant b_n<x_n, \quad (a_n,b_n)=1,$$

使得(因ξ_0为无理数)

$$0<y_n=|\xi_0-a_n/b_n|<1/(b_nx_n)<1/b_n^2,$$

那么，取$x_{n+1}=y_n^{-1}$，由定理 7 知必有

$$1\leqslant b_{n+1}<x_{n+1},\qquad (a_{n+1},b_{n+1})=1,$$

使得(因ξ_0为无理数)

$$0<y_{n+1}=|\xi_0-a_{n+1}/b_{n+1}|<1/(b_{n+1}x_{n+1})<1/b_{n+1}^2.$$

这样，就得到了无穷多个有理分数a_n/b_n满足式(12)，且有

$$|\xi_0-a_{n+1}/b_{n+1}|<|\xi_0-a_n/b_n|,\qquad n=0,1,2,\cdots.$$

证毕。

请读者证明：定理 8 中的$b_n\to+\infty$。

习　题　四

1．设ξ_0是无理数，它的无限简单连分数是$\langle a_0,a_1,a_2,\cdots\rangle$，$h_n/k_n$是它的渐近分数，$\xi_n$是它的第 n 个完全商．证明：

(i) $a_{n+1}<\xi_{n+1}+k_{n-1}/k_n<a_{n+1}+2$，$n\geqslant 0$。

(ii) 存在正数$\lambda=\lambda_0$，使§4式(2)仅对有限个有理分数a/b成立的充要条件是存在正数A，使$a_n\leqslant A$，$n\geqslant 0$。

2．求出$\xi_0=\sqrt{2},(\sqrt{5}+1)/2,\sqrt{11},\sqrt{14}$的所有渐近分数，使得§4式(2)当$a/b$为这些渐近分数时，(i) 对 $\lambda=2$ 成立，(ii) $\lambda=\sqrt{5}$成立．此外，求出数列$\xi_{n+1}+k_{n-1}/k_n$，$n\geqslant 0$的所有极限点，及上极限(提示：利用§1习题一第 6 题及§3 习题三第13题)。

3．设ξ_0为无理数．对给定的$x\geqslant 1$，如何利用渐近分数来求a/b使定理 7 (取 $\alpha=\xi_0$)成立．并以$\xi_0=\sqrt{7},\sqrt{13},\sqrt{23}$, $x=10^2$, $10^3,10^4$为例，找出具体的a/b。

4．(i) 证明对任给的实数 $c>2$，一定存在无理数ξ，使得仅有有限个有理数h/k ($k\geqslant 1$)满足$|\xi-h/k|<1/k^c$。

(ii) 证明对任意实数 c，一定存在无理数ξ，使得有无限个有理数 h/k ($k\geqslant 1$)满足$|\xi-h/k|<1/k^c$。

(iii) ξ_0是无理数的充要条件是存在无限多个有理分数 a/b 使式(13)成立。

下面的第 5—12题是一组关于 Farey 分数的习题。利用它也可以来讨论无理数的有理逼近。Farey 分数本身是数论中一个十分有趣和有用的课题。

5. 用下面的方法来构造一张有理分数表：先在第一行(从左至右)写下0/1,1/1这两个分数。当在第$n-1$行的各个分数已经写好后，这样来写第 n 行的分数：先在第 n 行中依次重写下第 $n-1$行中的全部分数，当这些分数中的任意相邻的两个分数a/b, a'/b'，如果满足$b+b'\leqslant n$时，就在(第 n 行的)这两个分数之间加写上分数$(a+a')/(b+b')$。这张表通常称为**Farey分数表**，它的第 n 行中的所有分数称为**第n阶 Farey 数列**。显见，这张表可以无限制编造下去。第342页列出了$n=7$时的表。

证明 Farey 分数表有以下性质：

(i) 如果 $a/b,a'/b'$是第 n 行中的两个相邻分数，且 a/b在 a'/b'的左边，那么，$a'b-ab'=1$。

(ii) 表中每个分数a/b都是既约的，即$(a,b)=1$。

(iii) 表中每一行的分数从左至右都是按它们的大小次序递增排列。

(iv) 设 $a/b<a'/b'$ 是同一行中的两个相邻分数，x,y 是整数，$y>0$。如果$a/b<x/y<a'/b'$，则$y\geqslant b+b'$。

(v) 第 n 行是由所有这样的既约有理分数 a/b 按大小顺序从左至右递增排列：$0\leqslant a/b\leqslant 1$，$(a,b)=1$，$1\leqslant b\leqslant n$。

6. 设 $a/b,c/d$ 是第 n 阶 Farey 数列中的两个相邻分数。证明：

(i) $|a/b-(a+c)/(b+d)|\leqslant 1/(b(n+1))$。

(ii) $|c/d-(a+c)/(b+d)|\leqslant 1/(d(n+1))$。

7. 设 ξ 是实数。利用上题证明：对任给的正整数 n，必有有理数 h/k 使得：$0<k\leqslant n$，$|\xi-h/k|\leqslant 1/(k(n+1))$。进而证

Farey 分数表 ($n=7$)

n	第 n 阶 Farey 数列
1	$\frac{0}{1}$ $\frac{1}{1}$
2	$\frac{0}{1}$ $\frac{1}{2}$ $\frac{1}{1}$
3	$\frac{0}{1}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{1}{1}$
4	$\frac{0}{1}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{1}{1}$
5	$\frac{0}{1}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{1}{2}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{1}{1}$
6	$\frac{0}{1}$ $\frac{1}{6}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{1}{2}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{5}{6}$ $\frac{1}{1}$
7	$\frac{0}{1}$ $\frac{1}{7}$ $\frac{1}{6}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{2}{7}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{3}{7}$ $\frac{1}{2}$ $\frac{4}{7}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{5}{7}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{5}{6}$ $\frac{6}{7}$ $\frac{1}{1}$

明：若ξ是无理数，则必有无穷多个不同的有理数h/k使得$|\xi-h/k|<1/k^2$。

8．设ξ是无理数，$0<\xi<1$。若ξ在第n阶Farey数列的两个相邻分数$a/b,c/d$之间，即$a/b<\xi<c/d$，证明：

(i) $|\xi-a/b|<1/(2b^2)$或$|\xi-c/d|<1(2d^2)$至少有一个成立，进而推出§4推论2。

(ii) $|\xi-a/b|<1/(\sqrt{5}b^2)$，$|\xi-c/d|<1/(\sqrt{5}d^2)$，或$|\xi-(a+c)/(b+d)|<1/(\sqrt{5}(b+d)^2)$至少有一个成立。进而推出§4推论5。

9．在第n阶Farey数列中，设$a/b,a'/b'$分别是与1/2左右相邻的分数。证明：$b=b'=1+2[(n-1)/2]$，即b是不超过n的最大奇数，且有$a+a'=b$。

10．设第n阶Farey数列的全体分数为$0=a_1/b_1<a_2/b_2<\cdots<a_k/b_k=1$。证明：

(i) $k=1+\sum_{m=1}^{n}\phi(n)$；

(ii) $\sum_{j=1}^{k}a_j/b_j=k/2$；

(iii) $\sum_{j=1}^{k-1}1/(b_jb_{j+1})=1$；

(iv) $\max_{1\leqslant j<k}(a_{j+1}/b_{j+1}-a_j/b_j)=1/n$，

$$\min_{1\leqslant j<k}(a_{j+1}/b_{j+1}-a_j/b_j)=1/n(n-1)。$$

11．设a,b,c,d是整数，$b>0,d>0$，$ad-bc=1$。再设$n=\max(b,d)$，a/b，c/d都属于第n阶Farey数列。证明：(i) a/b，c/d一定是第n阶Farey数列中的相邻分数。(ii) 它们在第$n+1$阶Farey数列中不一定相邻。

12．若$a/b,a'/b',a''/b''$为第n阶Farey数列中的三个相邻分数，证明：$a'/b'=(a+a'')/(b+b'')$。

§5 二次无理数与循环连分数

特殊形式的无理数的无限简单连分数应有特殊的形式与性质。本节将讨论所谓二次无理数的无限简单连分数，并在下一节利用它的性质来解Pell 方程。我们先来讨论二次无理数。

一个复数α称为**二次无理数**，如果α是某个整系数二次方程

$$\begin{cases} ax^2+bx+c=0, \\ \text{判别式} b^2-4ac \text{不是平方数} \end{cases} \tag{1}$$

的根。方程(1)有两个不同的根：

$$-b/(2a)+\sqrt{b^2-4ac}/(2a), \quad -b/(2a)-\sqrt{b^2-4ac}/(2a). \tag{2}$$

α必为其中之一。当二次无理数α为实数时，就称为**实二次无理数**。由式(2)知，α是实二次无理数当且仅当

$$b^2-4ac>0. \tag{3}$$

定理1 α是二次无理数的充要条件是存在非平方数的整数d，及有理数r,s，$s\neq 0$，使得

$$\alpha=r+s\sqrt{d}. \tag{4}$$

此外，α是实二次无理数的充要条件是$d>0$。

证 必要性 设α满足二次方程(1)。α必为式(2)给出的两个数中的一个，因此可取$d=b^2-4ac$，$r=-b/(2a)$，$s=1/(2a)$或$-1/(2a)$，即得式(4)。α为实数时必有$d>0$。

充分性 设α由式(4)给出。显见，α满足二次方程

$$(x-(r+s\sqrt{d}))(x-(r-s\sqrt{d}))=0,$$

即

$$x^2-2rx+(r^2-ds^2)=0.$$

表$r=h/l$，$s=k/l$，l,h,k为整数，$l>0$，$k\neq 0$，方程变为

$$l^2x^2-2lhx+(h^2-dk^2)=0. \tag{5}$$

它的判别式等于

$$(2lh)^2-4l^2(h^2-dk^2)=(2lk)^2d, \tag{5}$$

由 d 不是平方数就推出这判别式也不是平方数，所以 α 是二次无理数。当$d>0$时α为实数。证毕。

由于非平方数 d 必可表为(为什么)

$$d=n_1^2m, \tag{6}$$

n_1是正整数，$m\neq 0,1$且无平方因数。反过来，这样的 d 一定是非平方数。因此，由定理 1 立即推出：

推论2 当要求定理 1 中的整数 $d\neq 0,1$，且无平方因数时，定理 1 仍然成立。

定理3 设整数 d 不是平方数。那么，形如 $r+s\sqrt{d}$ (r,s 是有理数)的数的和、差、积、商仍是这种形式的数。

证 设 $\alpha_1=r_1+s_1\sqrt{d}$，$\alpha_2=r_2+s_2\sqrt{d}$，r_1,r_2,s_1,s_2 是有理数。我们有

$$\alpha_1\pm\alpha_2=(r_1\pm r_2)+(s_1\pm s_2)\sqrt{d},$$

$$\alpha_1\alpha_2=(r_1r_2+ds_1s_2)+(r_1s_2+s_1r_2)\sqrt{d},$$

以及当$\alpha_2\neq 0$，即$r_2,s_2\neq 0$时，$r_2^2-ds_2^2\neq 0$(为什么)，所以有

$$\frac{\alpha_1}{\alpha_2}=\frac{(r_1+s_1\sqrt{d})(r_2-s_2\sqrt{d})}{(r_2+s_2\sqrt{d})(r_2-s_2\sqrt{d})}$$

$$=\frac{(r_1r_2-ds_1s_2)}{r_2^2-ds_2^2}+\frac{(s_1r_2-r_1s_2)}{r_2^2-ds_2^2}\sqrt{d}.$$

这就证明了所要的结论。

设整数 d 不是平方数，r,s是有理数。我们把

$$\alpha=r+s\sqrt{d},\qquad \alpha'=r-s\sqrt{d} \tag{7}$$

称为是共轭数，也说α'是α的**共轭数**。当 $s=0$时，$\alpha=\alpha'=r$都是有理数。当$s\neq 0$时，由定理 1 的证明知，α,α'都是二次无理数，

且是判别式不是平方数的整系数二次方程(5)的两个根。反过来，满足这样的二次方程(1)的两个根由式(2)给出，是一对共轭数。显见，α'的共轭数是α，以及对给定的非平方数d，形如$r+s\sqrt{d}$的数的和、差、积及商的共轭数就等于这些数的共轭数的和、差、积及商(证明留给读者)。

下面来讨论循环连分数。设无限简单连分数

$$\xi_0=\langle a_0,a_1,a_2,\cdots\rangle. \tag{8}$$

如果存在$m\geqslant 0$，使得对这个m存在正整数k，使得当$n\geqslant m$时总有

$$a_{n+k}=a_n, \tag{9}$$

那么，ξ_0就称为**循环简单连分数**，简称**循环连分数**；如果可取$m=0$使式(9)成立，则ξ_0就称为**纯循环简单连分数**，简称**纯循环连分数**。

例如，$\langle 4,1,2,5,3,2,5,3,2,5,3,\cdots\rangle$是循环连分数，因为只要取$m\geqslant 2$，及正整数$k$满足$3|k$时，式(9)一定成立，所以$m$及$k$的取法不是唯一的。但$m$不能取0，所以它不是纯循环连分数。再如，

$$\langle 2,5,3,2,5,3,2,5,3,\cdots\rangle,$$
$$\langle 5,3,2,5,3,2,5,3,2,\cdots\rangle$$

都是纯循环连分数，因为$m=0$时，只要取正整数k满足$3|k$时，式(9)一定成立，所以k的取法不是唯一的。为简便起见，我们把有式(9)成立的ξ_0记作

$$\xi_0=\langle a_0,\cdots,a_{m-1},\overline{a_m,\cdots,a_{m+k-1}}\rangle. \tag{10}$$

这样就有

$$\begin{aligned}\langle 4,1,2,5,3,2,5,3,\cdots\rangle&=\langle 4,1,\overline{2,5,3}\rangle\\&=\langle 4,1,2,\overline{5,3,2}\rangle\\&=\langle 4,1,\overline{2,5,3,2,5,3}\rangle\\&=\langle 4,1,2,5,\overline{3,2,5}\rangle.\end{aligned}$$

所以形如式(10)的表示式不是唯一的。

显见，存在某个$m\geqslant 0$使式(9)成立与存在某个m使ξ_m是纯循环连分数是一回事，这里

$$\xi_j=\langle a_j,a_{j+1},\cdots\rangle. \tag{11}$$

此外，当式(9)对某个m成立，则对任意的$m'\geqslant m$式(9)也成立。这样，当ξ_0是循环连分数时，必有最小的m，设为$m_0\geqslant 0$，使得式(9)成立，当$m\geqslant m_0$时式(9)一定成立，当$m<m_0$时式(9)不可能成立。也就是说必有$m_0\geqslant 0$使得$m\geqslant m_0$时，ξ_m是纯循环连分数，而$m<m_0$时，ξ_m一定不是纯循环连分数。这样，由§3式(8)知，每个循环连分数必可唯一地表为

$$\xi_0=\langle a_0,a_1,a_2,\cdots\rangle=\langle a_0,\cdots,a_{m_0-1},\ \xi_{m_0}\rangle, \tag{12}$$

这里ξ_{m_0}是纯循环连分数，而任一$\xi_m(m<m_0)$一定不是纯循环连分数，ξ_{m_0}称为是ξ_0的**最大纯循环部分**。

当ξ_0是纯循环连分数时，必有正整数k，使

$$a_{n+k}=a_n,\qquad n\geqslant 0. \tag{13}$$

我们把使上式成立的最小的正整数k称为**纯循环连分数ξ_0的周期**，记作l。一般的，当ξ_0是循环连分数时，我们把唯一的表达式(12)中的纯循环连分数ξ_{m_0}的周期称为ξ_0的**周期**。这样，每个循环连分数ξ_0必可唯一的表为

$$\begin{aligned}\xi_0&=\langle a_0,\cdots,a_{m_0-1},\langle\overline{a_{m_0},\cdots,\ a_{m_0+l-1}}\rangle\rangle\\&=\langle a_0,\cdots,\ a_{m_0-1},\ \overline{a_{m_0},\cdots,\ a_{m_0+l-1}}\rangle,\end{aligned} \tag{14}$$

这里$\xi_{m_0}=\langle\overline{a_{m_0},\cdots,a_{m_0+l-1}}\rangle$是$\xi_0$的最大纯循环部分，$l$是它的周期。这样

$$\langle 4,1,2,5,3,2,5,3,2,5,3,\cdots\rangle=\langle 4,1,\overline{2,5,3}\rangle,$$
$$\langle 2,5,3,2,5,3,2,5,3,\cdots\rangle=\langle\overline{2,5,3}\rangle,$$

就是形如(14)的表示式。它们的周期都是3。

定理4 (i) ξ_0是纯循环连分数的充要条件是存在$k\geqslant 1$使得

$$\xi_0=\xi_k, \tag{15}$$

(ii) 设 ξ_0 是纯循环连分数，周期为 l。那么，式(15)成立的充要条件是 $l|k$。

(iii) 设 ξ_0 是纯循环连分数，那么对任意的 $m\geqslant 0$，ξ_m 也是纯循环连分数，且周期都相同。

(iv) 设 ξ_0 是循环连分数。那么对任意的 $m'\geqslant 0$，$\xi_{m'}$ 也是循环连分数，且周期都相同。

证 由定义知，ξ_0是纯循环连分数就是有式(13)成立。由§3推论3知，式(13)等价于式(15)。这就证明了(i)。当纯循环连分数 ξ_0 的周期为 l 时，若 $k\geqslant 1$ 使式(13)成立，则 $k\geqslant l$。因而 $k=ql+l'$，$q\geqslant 0$，$0\leqslant l'<l$，所以对任意的$n\geqslant 0$有

$$a_n=a_{n+k}=a_{n+l'+ql}=a_{n+l'}.$$

由此及 l 的最小性就推出$l'=0$，即$l|k$。反过来，若 $l|k\geqslant 1$，则显然有式(13)成立。这就证明了式(13)与 $l|k$是等价的。由此及(i)就证明了(ii)。下面来证(iii)。前面已经指出，存在某个m使式(9)成立就是说 ξ_m 是纯循环连分数。当 ξ_0 是纯循环连分数时式(13)成立，因而对任意取定的$m\geqslant 0$有式(9)成立，因而ξ_m是纯循环连分数。设ξ_0和ξ_m的周期分别为 l 和 l_1。显见，使式(13)成立的k一定使式(9)(对所取的这个m)也成立，而 l 是使式(13)成立的最小的 k，l_1 是使式(9)(对所取的这个m)成立的最小的 k，因此$l_1\leqslant l$。另一方面，必有正整数 q，使 $ql\geqslant m$，这时必有 $\xi_{ql}=\xi_0$。以ξ_m和ξ_{ql}代替上面的ξ_0和 ξ_m作同样的讨论可得 $l\leqslant l_1$。所以 $l=l_1$。这就证明了(iii)。当 ξ_0是循环连分数时，由定义即知对任意的$m'\geqslant 0$，$\xi_{m'}$ 也是循环连分数。利用(iii)即可推出所有 $\xi_{m'}$ $(m'\geqslant 0)$的周期相同(具体推导留给读者)。这就证明了(iv)。证毕。

循环连分数ξ_0的值是很容易求出的，例如，§3的例1，例2及例3，其方法是先求出它的纯循环部分 ξ_{m_0}(见式(14))，然后通过计算有限连分数$\langle a_0,\cdots,a_{m_0-1},\xi_{m_0}\rangle$就求得$\xi_0$的值。下面来举个例子。

例 1 求 $\xi_0=\langle -1,1,4,\overline{3,1,1,1,3,7}\rangle$的值.

解 ξ_0的最大纯循环部分是 $\xi_3=\langle\overline{3,1,1,1,3,7}\rangle$。$\xi_3$满足

$$\xi_3=\langle 3,1,1,1,3,7,\xi_3\rangle.$$

先分别计算$\langle 3,1,1,1,3\rangle$及$\langle 3,1,1,1,3,7\rangle$。我们有

$$\begin{aligned}\langle 3,1,1,1,3\rangle&=\langle 3,1,1,4/3\rangle=\langle 3,1,7/4\rangle\\&=\langle 3,11/7\rangle=40/11.\end{aligned}$$

$$\langle 3,1,1,1\rangle=\langle 3,1,2\rangle=\langle 3,3/2\rangle=11/3.$$

利用 §3式(17)得

$$\langle 3,1,1,1,3,7\rangle=(7\cdot 40+11)/(7\cdot 11+3)=291/80,$$

以及

$$\xi_3=\langle 3,1,1,1,3,7,\xi_3\rangle=(291\xi_3+40)/(80\xi_3+11).$$

进而有$2\xi_3^2-7\xi_3-1=0$。由此及 $\xi_3>1$得

$$\xi_3=(7+\sqrt{57})/4.$$

因此

$$\begin{aligned}\xi_0&=\langle -1,1,4,(7+\sqrt{57})/4\rangle\\&=\langle -1,1,(\sqrt{57}+1)/2\rangle\\&=\langle -1,(\sqrt{57}+3)/(\sqrt{57}+1)\rangle\\&=(3-\sqrt{57})/24.\end{aligned}$$

定理5 (i) 纯循环连分数 ξ_0 的值一定是实二次无理数,$\xi_0>1$,以及它的共轭数 ξ_0' 满足 $-1<\xi_0'<0$。

(ii) 循环连分数的值是实二次无理数。

证 (i) 设纯循环连分数 ξ_0 的周期为 l .因而有

$$\xi_0=\langle a_0,\cdots,a_{l-1},\xi_0\rangle.$$

由 $a_0=a_l\geqslant 1$ 知 $\xi_0>1$.由 §3式(17)知

$$\xi_0=\frac{h_{l-1}\xi_0+h_{l-2}}{k_{l-1}\xi_0+k_{l-2}},$$

这里 h_n,k_n 由 §2式(2)给出。因此 ξ_0 满足整系数二次方程

$$f(x)=k_{l-1}x^2+(k_{l-2}-h_{l-1})x-h_{l-2}=0.$$

由于无限简单连分数 ξ_0 的值一定是无理数，所以上述二次方程的判别式一定不是平方数①，因而 ξ_0 是实二次无理数．由于 $a_j\geqslant 1$，$j\geqslant 0$，所以由 § 2式(2)知

$$f(0)=-h_{l-2}\leqslant -1,\quad l\geqslant 1.$$

$$\begin{aligned}f(-1)&=(k_{l-1}-k_{l-2})+(h_{l-1}-h_{l-2})\\&=k_{l-2}(a_{l-1}-1)+h_{l-2}(a_{l-1}-1)\\&\quad+k_{l-3}+h_{l-3}\geqslant 1,\quad l\geqslant 1.\end{aligned}$$

所以 ξ_0 的共轭数 ξ_0' 即 $f(x)=0$ 的另一根必满足 $-1<\xi_0'<0$．

(ii) 由式(12)及 § 3式(17)知

$$\xi_0=\langle a_0,\cdots,a_{m_0-1},\xi_{m_0}\rangle$$

$$=\frac{h_{m_0-1}\xi_{m_0}+h_{m_0-2}}{k_{m_0-1}\xi_{m_0}+k_{m_0-2}}.$$

由(i)知 ξ_{m_0} 是实二次无理数，由此利用定理 1、定理 3 、及 ξ_0 是无理数，从上式就推出 ξ_0 是实二次无理数．证毕．

本节主要证明定理 5 的逆定理也成立．

定理6 设 ξ_0 是实二次无理数．那么，

(i) ξ_0 的无限简单连分数表示式一定是一个循环连分数．

(ii) 设 ξ_0' 是 ξ_0 的共轭数．若满足 $\xi_0>1$，$-1<\xi_0'<0$，则 ξ_0 的无限简单连分数表示式一定是一个纯循环连分数．

证 由定理 1 知，实二次无理数 ξ_0 一定可表为（为什么）

$$\xi_0=(\sqrt{d}+c)/q,\quad d,q,c\in\boldsymbol{Z},d>1\text{ 是非平方数}.$$

但这时并不一定满足条件 $q\mid d-c^2$．当用 § 3定理 4 的方法来求 ξ_0 的无限简单连分数表示式时，如果有这条件成立则可使求表示式的过程简单．注意到表达式

$$\xi_0=(\sqrt{dq^2}+c|q|)/(q|q|)$$

就满足这条件，因此，ξ_0 一定可表为：

① 可以利用 h_j,k_j 的性质，直接证明方程的判别式不是平方数，请读者自证．

$$\xi_0=(\sqrt{d}+c_0)/q_0,\quad q_0|d-c_0^2,\tag{16}$$
这里 $d>1$ 是非平方数。现在用§3定理4的方法来求 ξ_0 的无限简单连分数表示。以下符号均和§3定理4相同。

先来证明所有的 ξ_j 均可表为形如(16)的形式。我们有 $a_0=[\xi_0]$，以及由式(16)得
$$\xi_1^{-1}=\xi_0-a_0=\frac{d-(a_0q_0-c_0)^2}{q_0(\sqrt{d}+(a_0q_0-c_0))}.\tag{17}$$
取
$$c_1=a_0q_0-c_0,\tag{18}$$
由 $q_0|d-c_0^2$ 就推出 $q_0|d-c_1^2$，设
$$q_1q_0=d-c_1^2,\tag{19}$$
就得 ξ_1 可表为式(16)的形式：
$$\xi_1=(\sqrt{d}+c_1)/q_1,\quad q_1|d-c_1^2.\tag{20}$$
继续依此递推定义：若对 $j(\geqslant 0)$ 有
$$\xi_j=(\sqrt{d}+c_j)/q_j,\quad q_j|d-c_j^2,\tag{21}$$
则由 $a_j=[\xi_j]$ 及取
$$c_{j+1}=a_jq_j-c_j,\quad q_{j+1}q_j=d-c_{j+1}^2\tag{22}$$
得（注意：d 不是平方数，所以 q_j 均不为零）
$$\xi_{j+1}=(\sqrt{d}+c_{j+1})/q_{j+1},\quad q_{j+1}|d-c_{j+1}^2.\tag{23}$$
这就证明了所要的结论，即式(21)对所有 $j\geqslant 0$ 成立，c_j，q_j 由式(22)给出。为了证明 ξ_0 是循环连分数，只要证明存在 $k>h\geqslant 0$ 使 $\xi_h=\xi_k$（为什么），由 ξ_j 有式(21)的表示式知，这就等价于要证明：存在 $k>h\geqslant 0$ 使
$$q_k=q_h,\quad c_k=c_h.\tag{24}$$

现在先来证明式(24)可由下面的结论推出：存在 $j_0\geqslant 0$，使得当 $j\geqslant j_0$ 时
$$q_j>0.\tag{25}$$
若式(25)成立，则当 $j\geqslant j_0$ 时，由式(22)第二式知：

$$0<q_j q_{j+1}=d-c_{j+1}^2\leqslant d.$$

因此，$\{q_j\}$只取有限多个值，$\{c_j\}$也只取有限多个值。由此容易推出式(24)(留给读者)，这就证明了(i)。

式(25)的证明 由§3式(17)$(n=j-1)$解出ξ_j得

$$\xi_j=-\frac{k_{j-2}}{k_{j-1}}\left(\frac{\xi_0-r^{(j-2)}}{\xi_0-r^{(j-1)}}\right),\quad j\geqslant 2. \tag{26}$$

这里$r^{(n)}=\langle a_0,\cdots,a_n\rangle=h_n/k_n$。设$\xi_n'$是$\xi_n$的共轭数。对取定的非平方数$d$，一些形如$r+s\sqrt{d}$($r,s$有理数)的二次无理数作四则运算后的值的共轭数等于这些数的共轭数作四则运算后所得的值(证明留给读者)，所以由上式及式(21)得

$$\xi_j'=-\frac{k_{j-2}}{k_{j-1}}\left(\frac{\xi_0'-r^{(j-2)}}{\xi_0'-r^{(j-1)}}\right)=\frac{-\sqrt{d}+c_j}{q_j}. \tag{27}$$

由于当$j\to\infty$时$r^{(j)}\to\xi_0$，以及$\xi_0\neq\xi_0'$(为什么)，所以必有$j_0\geqslant 2$，使$j\geqslant j_0$时$\xi_j'<0$(为什么)。由此及$\xi_j\geqslant 1(j\geqslant 1)$，再利用上式及式(21)得：

$$1<\xi_j-\xi_j'=2\sqrt{d}/q_j,\quad j\geqslant j_0. \tag{28}$$

$$0<q_j<2\sqrt{d},\quad j\geqslant j_0. \tag{29}$$

这就证明了式(25)，而且也同时证明了q_j只取有限多个值。这就证明了(i)。

下面来证明(ii)。设$\xi_0=\langle a_0,a_1,\cdots\rangle$。由$\xi_0>1$知$a_j\geqslant 1,j\geqslant 0$。(i)已经证明必有$k>h\geqslant 0$使

$$\xi_h=\xi_k. \tag{30}$$

若$h=0$，则由此即知ξ_0的无限简单连分数表示式是纯循环的。若$h>0$，我们来证明由式(30)可推出

$$\xi_{h-1}=\xi_{k-1}. \tag{31}$$

因而，依次可得$\xi_{h-2}=\xi_{k-2},\cdots,\xi_0=\xi_{k-h}$，这也证明了所要的结论。

由条件知对所有的$j\geqslant 0$有$\xi_j>1$。现来证明当$j\geqslant 0$时，

$$-1<\xi'_j<0.\qquad(32)$$

由条件知，$j=0$ 时成立。假设 $j=n(\geqslant 0)$ 时成立。当 $j=n+1$ 时

$$\xi'_{n+1}=1/(\xi'_n-a_n),$$

利用 $a_n\geqslant 1(n\geqslant 0)$ 和归纳假设，从上式就推出式（32）对 $j=n+1$ 成立。这就证明了式(32)对所有的 $j\geqslant 0$ 成立。

由于 $a_j=\xi_j-1/\xi_{j+1}$，所以 $a_j=\xi'_j-1/\xi'_{j+1}$。由此及式(32)得

$$0<-a_j-1/\xi'_{j+1}<1,$$

因而得

$$a_j=[-1/\xi'_{j+1}],\quad j\geqslant 0.\qquad(33)$$

由式(30)可得 $\xi'_h=\xi'_k$，当 $h\geqslant 1$ 时，由此及式(33)就得

$$a_{h-1}=a_{k-1}.$$

由此及式(30)就得到

$$\xi_{h-1}=a_{h-1}+1/\xi_h=a_{k-1}+1/\xi_k=\xi_{k-1},$$

即式(31)成立。证毕。

例 2 求 $\xi_0=(\sqrt{14}+1)/2$ 的循环连分数。

解 我们按定理 6 的方法来求，即要求出最小的 $k>h\geqslant 0$ 使 $\xi_h=\xi_k$，即式(24)成立，为使条件(16)成立，ξ_0 应表为

$$\xi_0=(\sqrt{56}+2)/4,\quad d=56,$$
$$c_0=2,\quad q_0=4,\quad a_0=[\xi_0]=2.$$

现按递推公式(22)及(23)来求 c_j,q_j,ξ_j,a_j。

$$\begin{aligned}
&c_0=2, && q_0=4,\\
&\xi_0=(\sqrt{56}+2)/4, && a_0=2.\\
&c_1=2\cdot 4-2=6, && q_1=(56-6^2)/4=5,\\
&\xi_1=(\sqrt{56}+6)/5, && a_1=2.\\
&c_2=2\cdot 5-6=4, && q_2=(56-4^2)/5=8,\\
&\xi_2=(\sqrt{56}+4)/8, && a_2=1.\\
&c_3=1\cdot 8-4=4, && q_3=(56-4^2)/8=5,\\
&\xi_3=(\sqrt{56}+4)/5, && a_3=2.
\end{aligned}$$

$c_4 = 2 \cdot 5 - 4 = 6$, $\qquad q_4 = (56 - 6^2)/5 = 4$,

$\xi_4 = (\sqrt{56} + 6)/4$, $\qquad a_4 = 3$.

$c_5 = 3 \cdot 4 - 6 = 6$, $\qquad q_5 = (56 - 6^2)/4 = 5$,

$\xi_5 = (\sqrt{56} + 6)/5$, $\qquad a_5 = 2$.

这就求出了 $h = 1, k = 5$ 是最小的值使 $\xi_k = \xi_h$。因而得到

$$\xi_0 = (\sqrt{14} + 1)/2 = \langle 2, \overline{2, 1, 2, 3} \rangle.$$

对定理 6 的方法稍作修改，可以得到另一种具体算法，当求 $c_j, q_j (j \geqslant 2)$ 时，运算中不出现 d 也不需作除法。由式(22)知

$$q_{j+1} q_j + c_{j+1}^2 = q_j q_{j-1} + c_j^2, \quad c_{j+1} + c_j = a_j q_j, \quad j \geqslant 1,$$

因而有

$$\begin{cases} q_{j+1} = q_{j-1} + (c_j^2 - c_{j+1}^2)/q_j \\ \qquad\quad = q_{j-1} + (c_j - c_{j+1}) a_j, \quad j \geqslant 1. \\ c_{j+1} = a_j q_j - c_j. \end{cases} \tag{34}$$

这样，先求出 q_0, c_0, a_0 及 q_1, c_1, a_1，然后用式(34)求 $q_j, c_j (j \geqslant 2)$。而 a_j 仍用原来公式 $[\xi_j] = [(\sqrt{d} + c_j)/q_j]$。下面举例说明这一方法。

例 3 求 $\xi_0 = \sqrt{73}$ 的循环连分数。

解 为使条件(16)成立，ξ_0 应表为

$$\xi_0 = (\sqrt{73} + 0)/1, \quad q_0 = 1, c_0 = 0, d = 73.$$

$a_0 = [\sqrt{73}] = 8$. 利用式(22)求得

$$c_1 = 8 \cdot 1 - 0 = 8, \quad q_1 = (73 - 8^2)/1 = 9,$$

$$\xi_1 = (\sqrt{73} + 8)/9, \quad a_1 = 1.$$

下面按式(34)来求。

$c_0 = 0$, $\qquad q_0 = 1$,

$\xi_0 = (\sqrt{73} + 0)/1$, $\qquad a_0 = 8$.

$c_1 = 8$, $\qquad q_1 = 9$,

$\xi_1 = (\sqrt{73} + 8)/9$, $\qquad a_1 = 1$.

$c_2 = 1\cdot 9 - 8 = 1$, $q_2 = 1 + (8-1)\cdot 1 = 8$,

$\xi_2 = (\sqrt{73}+1)/8$, $a_2 = 1$.

$c_3 = 1\cdot 8 - 1 = 7$, $q_3 = 9 + (1-7)\cdot 1 = 3$,

$\xi_3 = (\sqrt{73}+7)/3$, $a_3 = 5$.

$c_4 = 5\cdot 3 - 7 = 8$, $q_4 = 8 + (7-8)\cdot 5 = 3$,

$\xi_4 = (\sqrt{73}+8)/3$, $a_4 = 5$.

$c_5 = 5\cdot 3 - 8 = 7$, $q_5 = 3 + (8-7)\cdot 5 = 8$,

$\xi_5 = (\sqrt{73}+7)/8$, $a_5 = 1$.

$c_6 = 1\cdot 8 - 7 = 1$, $q_6 = 3 + (7-1)\cdot 1 = 9$,

$\xi_6 = (\sqrt{73}+1)/9$, $a_6 = 1$.

$c_7 = 1\cdot 9 - 1 = 8$, $q_7 = 8 + (1-8)\cdot 1 = 1$,

$\xi_7 = (\sqrt{73}+8)/1$, $a_7 = 16$.

$c_8 = 16\cdot 1 - 8 = 8$, $q_8 = 9 + (8-8) = 9$,

$\xi_8 = (\sqrt{73}+8)/9$, $a_8 = 1$.

这就求出了 $\xi_8 = \xi_1$，因而得

$$\xi_0 = \sqrt{73} = \langle 8, \overline{1,1,5,5,1,1,16} \rangle.$$

设 $d>1$ 是非平方数，ξ_0 由式 (16) 给出。由定理 6 知 ξ_j 可由式(21)表出，但另一方面 ξ_0 和 ξ_j 之间又有一般的关系式——§3 式(17)。因此，由这两个关系式可推出 $\{c_n\}$，$\{q_n\}$ 和 $\{h_n\}$，$\{k_n\}$ 之间的关系，下面的定理就是刻画这种关系。

定理7 设 ξ_0 由式(16)给出，

$$\xi_0 = \langle a_0, a_1, a_2, \cdots \rangle.$$

再设 h_n, k_n 由 §2 式(2)给出，c_n, q_n 由式(21)给出。那么有

$$(-1)^{n+1} c_n = (q_0 h_{n-1} h_{n-2} - c_0(h_{n-1}k_{n-2} + h_{n-2}k_{n-1})) - \frac{d-c_0^2}{q_0} k_{n-1}k_{n-2}, \quad n \geqslant 0. \tag{35}$$

$$(-1)^n q_0 q_n = (q_0 h_{n-1} - c_0 k_{n-1})^2 - d k_{n-1}^2, \quad n \geqslant 0. \tag{36}$$

特别地，当 $c_0=0, q_0=1$，即 $\xi_0=\sqrt{d}$ 时有

$$(-1)^{n+1}c_n=h_{n-1}h_{n-2}-dk_{n-1}k_{n-2}, \quad n\geqslant 0. \tag{37}$$

$$(-1)^n q_n=h_{n-1}^2-dk_{n-1}^2. \quad n\geqslant 0. \tag{38}$$

证 由§3式(17)得

$$\xi_0=(h_{n-1}\xi_n+h_{n-2})/(k_{n-1}\xi_n+k_{n-2}), \quad n\geqslant 0.$$

ξ_0, ξ_n 用表达式(21)代入得到

$$\frac{\sqrt{d}+c_0}{q_0}=\frac{h_{n-1}(\sqrt{d}+c_n)+h_{n-2}q_n}{k_{n-1}(\sqrt{d}+c_n)+k_{n-2}q_n}, \quad n\geqslant 0.$$

$$(\sqrt{d}+c_0)(k_{n-1}(\sqrt{d}+c_n)+k_{n-2}q_n)$$

$$=q_0(h_{n-1}(\sqrt{d}+c_n)+h_{n-2}q_n), \quad n\geqslant 0.$$

由上式比较系数得

$$(q_0h_{n-1}-c_0k_{n-1})c_n+(q_0h_{n-2}-c_0k_{n-2})q_n=dk_{n-1}, \quad n\geqslant 0,$$

$$k_{n-1}c_n+k_{n-2}q_n=(q_0h_{n-1}-c_0k_{n-1}), \quad n\geqslant 0.$$

由以上两式解出 q_n, c_n，利用§2式(5)简化后即得式(35)及(36)。由于 $q_0|d-c_0^2$，所以式(36)的右边可被 q_0 整除。证毕。

对特殊的实二次无理数，q_n 应有特殊的性质。下面来讨论最简单的情形。

定理8 设 $d>1$ 是非平方数，$\xi_0=\sqrt{d}+[\sqrt{d}]$。再设 ξ_j, a_j 同§3定理4，以及 c_j, q_j 是由定理6给出的 ξ_j 的表示式(21)确定。那么，

(i) $q_j=1$ 的充要条件是 $l|j$，这里 l 是 ξ_0 的纯循环连分数的周期。

(ii) 对任意的 $j\geqslant 0, q_j\neq -1$。

证 设 ξ_0 的共轭数是 ξ_0'。我们有

$$\xi_0>1, \quad -1<\xi_0'=-\sqrt{d}+[\sqrt{d}]<0.$$

所以由定理6知 ξ_0 的无限简单连分数是纯循环的。由定理4(iii)知任一 ξ_j 的无限简单连分数都是纯循环的。若 $q_j=1$，则由式(21)

知$\xi_j=\sqrt{d}+c_j$。因而由定理 5 知，必有

$$\xi_j>1,\quad -1<\xi_j'=-\sqrt{d}+c_j<0.$$

因此，必有 $c_j=[\sqrt{d}]$，即 $\xi_j=\xi_0$。这就证明了 $q_j=1$的充要条件是 $\xi_j=\xi_0$。由此及定理 4(ii)就证明了(i)。

下面来证(ii)。若有 $j\geqslant 0$ 使 $q_j=-1$，则 $\xi_j=-\sqrt{d}-c_j$。由于前面已指出 ξ_j 的无限简单连分数一定是纯循环的，故由定理 5 (i)知，必须有

$$\xi_j=-\sqrt{d}-c_j>1,\quad -1<\xi_j'=\sqrt{d}-c_j<0,$$

即有

$$-\sqrt{d}-1>c_j>\sqrt{d},$$

这是不可能的。所以对任意的 $j\geqslant 0$，$q_j\neq -1$。证毕。

推论9 在定理 8 的条件和符号下，

$$\xi_0=\sqrt{d}+[\sqrt{d}]=\langle\overline{a_0,a_1,\cdots,a_{l-1}}\rangle,\quad a_0=2[\sqrt{d}].\quad (39)$$

以及

$$\xi_0=\sqrt{d}=\langle[\sqrt{d}],\overline{a_1,\cdots,a_{l-1},a_0}\rangle.\quad (40)$$

此外，若设 $\bar{\xi}_0=\langle\bar{a}_0,\bar{a}_1,\bar{a}_2,\cdots\rangle$，$\bar{\xi}_j=\langle\bar{a}_j,\bar{a}_{j+1},\cdots\rangle$，以及

$$\bar{\xi}_j=(\sqrt{d}+\bar{c}_j)/\bar{q}_j,\quad \bar{c}_{j+1}=\bar{a}_j\bar{q}_j-\bar{c}_j,$$

$$\bar{q}_{j+1}\bar{q}_j=d-\bar{c}_{j+1}^2,\quad j\geqslant 0,$$

$\bar{c}_0=0$，$\bar{q}_0=1$。那么，$\bar{a}_0=[\sqrt{d}]$，

$$\bar{\xi}_j=\xi_j,\quad \bar{a}_j=a_j,\quad \bar{c}_j=c_j,\quad j\geqslant 1,$$

$$\bar{q}_j=q_j,\quad j\geqslant 0,$$

以及 $\bar{q}_j=1$ 的充要条件是 $l\mid j$，对任意的 $j\geqslant 0$，$\bar{q}_j\neq -1$。

利用 $\bar{\xi}_1=\xi_1$，从定理 8 立即推出所有结论，详细论证留给读者。例 3 给出了定理 8 的具体例子。

定理 7 和定理 8 是应用连分数理论解 Pell 方程的基础。

习 题 五

1．设$\langle a_0, a_1, a_2, \cdots\rangle$是循环连分数，周期为$l$，$h_n/k_n$是它的渐近分数，$\xi_n=\langle a_n, a_{n+1}, \cdots\rangle$。证明：

(i) $\xi_{n+1}+k_{n-1}/k_n=\langle \xi_{n+1}, a_n, \cdots, a_1\rangle$。

(ii) 数列$\xi_{n+1}+k_{n-1}/k_n\,(n\geqslant 0)$的极限点至多有$l$个，它们是

$$\lambda_k=\langle \overline{a_k, \cdots, a_{k+l-1}}\rangle+(\langle \overline{a_{k-1}, \cdots, a_{k-l}}\rangle)^{-1},$$

$k=m_0+l, \cdots, m_0+2l-1$，这里假定$\xi_0$由§5式(14)给出。

(iii) 对$\xi_0=\langle 2,5,1,\overline{1,2}\rangle, \langle 0,5,8,6,\overline{1,1,1,4}\rangle, \langle \overline{2,1,3,1,2,8}\rangle$，分别求出(ii)中的各个极限点。

2．求以下二次无理数的循环连分数表示式，它的纯循环部分及周期。

(i) $(5+\sqrt{37})/3$，(ii) $\sqrt{43}$，(iii) $(6+\sqrt{43})/7$，

(iv) $\sqrt{80}+8$，(v) $(3+\sqrt{7})/2$．(vi) $\sqrt{26/5}$。

3．设二次无理数$\alpha=(a+\sqrt{d})/b$，a, b, d是整数，$b>0$．d是非平方数．α'是α的共轭数．证明：有$\alpha>1$，$-1<\alpha'<0$成立的充要条件是：$0<a<\sqrt{d}$，$\sqrt{d}-a<b<\sqrt{d}+a$．进而求出

(i) $a=[\sqrt{d}]$时所有满足$\alpha>1$，$-1<\alpha'<0$的α；

(ii) $b=1$时的所有这种α；

(iii) $a=1$时的所有这种α．

以$d=2,5,7,11,19,37$为例，具体说明以上结论。

4．用以下方法来证明定理6(i)．设实二次无理数ξ_0是$f(x)=ax^2+bx+c=0$的根，ξ_0的无限简单连分数是$\langle a_0, a_1, a_2, \cdots\rangle$．证明：

(i) $\xi_n=\langle a_n, a_{n+1}, \cdots\rangle$满足二次方程$A_nx^2+B_nx+C_n=0$，其中($h_n/k_n$是$\xi_0$的渐近分数)

$$A_n=ah_{n-1}^2+bh_{n-1}k_{n-1}+ck_{n-1}^2,$$

$$B_n=2ah_{n-1}h_{n-2}+b(k_{n-1}h_{n-2}+k_{n-2}h_{n-1})+2ck_{n-1}k_{n-2},$$

$$C_n = ah_{n-2}^2 + bh_{n-2}k_{n-2} + ck_{n-2}^2.$$

(ii) 对任意 $n\geqslant 0$, $B_n^2 - 4A_nC_n = b^2 - 4ac$.

(iii) 对 $n\geqslant 0$ 有

$$|A_n| < |2a\xi_0| + |a| + |b|, \quad |C_n| < |2a\xi_0| + |a| + |b|,$$

$$B_n^2 < 4(|2a\xi_0| + |a| + |b|)^2 + (b^2 - 4ac).$$

(iii) 至少有三个 $\xi_{n_1}, \xi_{n_2}, \xi_{n_3}$ 是同一个整系数二次方程 $Ax^2 + Bx + C = 0$ 的根。

5. 设 $\xi_0 = \langle \overline{a_0, a_1, \cdots, a_n} \rangle$, ξ_0' 是 ξ_0 的共轭数。证明:

$$-1/\xi_0' = \langle \overline{a_n, a_{n-1}, \cdots, a_0} \rangle.$$

6. 证明: 当且仅当 $d = a^2 + 1$ (a 是正整数) 时 $\sqrt{d}$ 的循环连分数的周期为 1, 且 $\sqrt{a^2+1} = \langle a, \overline{2a} \rangle$. 由此求 $\sqrt{101}$, $\sqrt{325}$, $\sqrt{2602}$ 的循环连分数。

7. 设整数 $a\geqslant 2$. 证明: (i) $\sqrt{a^2-1} = \langle a-1, \overline{1, 2a-2} \rangle$;

(ii) $\sqrt{a^2-a} = \langle a-1, \overline{2, 2a-2} \rangle$. 举例说明(i), (ii)的应用。

8. 设整数 $a\geqslant 3$. 证明:

(i) $\sqrt{a^2-2} = \langle a-1, \overline{1, a-2, 1, 2a-2} \rangle$.

(ii) $\sqrt{a^2+2} = \langle a, \overline{a, 2a} \rangle$. 具体举例说明(i), (ii)的应用。

9. 设 a 是奇数。证明:

(i) 当 $a>1$ 时, $\sqrt{a^2+4} = \langle a, \overline{(a-1)/2, 1, 1, (a-1)/2, 2a} \rangle$.

(ii) $a>3$ 时, $\sqrt{a^2-4} = \langle a-1, \overline{1, (a-3)/2, 2, (a-3)/2, 1, 2a-2} \rangle$. 具体举例说明(i), (ii)的应用。

10. 证明: $\sqrt{d}$ 的循环连分数周期等于 2 的充要条件是 $d = a^2 + b$, $b>1$, $b\,|\,2a$, 且 $\sqrt{a^2+b} = \langle a, \overline{2a/b, 2a} \rangle$. 举例说明这一结论的应用。

11. 设 l 是正整数。证明存在无穷多个 $\sqrt{d}$, 它的循环连分数的周期为 l.

12. 设 $\sqrt{d}$ 的循环连分数是

$$\langle [\sqrt{d}], \overline{a_1, \cdots, a_{l-1}, 2[\sqrt{d}]} \rangle,$$

l 是周期。证明：

$$\langle a_1, \cdots, a_{l-1}\rangle = \langle a_{l-1}, \cdots, a_1\rangle，即\ a_j = a_{l-j}, 1\leqslant j\leqslant l/2.$$

13．设 ξ_0 是二次无理数，它的循环连分数的周期为 l，h_n/k_n 是它的渐近分数。证明：

(i) 当 ξ_0 是纯循环连分数时，存在整数 $a,b,c,d, ad-bc=(-1)^l$，使得

$$\begin{pmatrix} h_{n+l} \\ k_{n+l} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} h_n \\ k_n \end{pmatrix}, \quad n\geqslant 0.$$

(ii) 当 ξ_0 是循环连分数由§5式(14)给出时，存在整数 $a,b,c,d,ad-bc=(-1)^l$，使得

$$\begin{pmatrix} h_{n+l} \\ k_{n+l} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} h_n \\ k_n \end{pmatrix}, \quad n\geqslant m_0.$$

14．设 $\sqrt{d}$ 的循环连分数同第13题，h_n/k_n 是它的渐近分数。证明：对正整数 m，当 $1\leqslant j\leqslant ml$ 时，

$$\begin{pmatrix} h_{ml-1} \\ k_{ml-1} \end{pmatrix} = k_{j-1}\begin{pmatrix} h_{ml-j} \\ k_{ml-j} \end{pmatrix} + k_{j-2}\begin{pmatrix} h_{ml-j-1} \\ k_{ml-j-1} \end{pmatrix}, \qquad (*)$$

及

$$\begin{pmatrix} dk_{ml-1} \\ h_{ml-1} \end{pmatrix} = h_{j-1}\begin{pmatrix} h_{ml-j} \\ k_{ml-j} \end{pmatrix} + h_{j-2}\begin{pmatrix} h_{ml-j-1} \\ k_{ml-j-1} \end{pmatrix}. \qquad (**)$$

进而推出

$$\begin{cases} k_{2ml-1} = k_{ml-1}(k_{ml} + k_{ml-2}) = 2h_{ml-1}k_{ml-1}, \\ h_{2ml-1} = h_{ml-1}^2 + dk_{ml-1}^2. \end{cases} \qquad (***)$$

15．设无理数 $\alpha = \langle \overline{a_0, a_1}\rangle, a_0 = ca_1$，及 β 是它的共轭数。再设 h_n/k_n 是 α 的渐近分数。证明：

$$h_n = c^{-[(n+1)/2]}\frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta}, \quad n\geqslant -2,$$

$$k_n = c^{-[(n+1)/2]}\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}, \quad n\geqslant -2.$$

16．设 $u_1, u_2, \cdots, u_n, \cdots$ 是 Fibonacci 数列，即 $u_1=u_2=1, u_{n+2}=u_{n+1}+u_n, n\geqslant 1$。证明：

$$u_n=\frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right\}, \quad n\geqslant 1.$$

§6　$x^2-dy^2=\pm 1$

这一节我们应用连分数理论来解不定方程

$$x^2-dy^2=1, \tag{1}$$

及

$$x^2-dy^2=-1, \tag{2}$$

这里 d 是非平方数，$d>1$。通常这类方程称为 Pell 方程，满足 $x>0, y>0$ 的解称为正解。

定理1　设 $\xi_0=\sqrt{d}$，它的循环连分数周期为 l，渐近分数为 h_n/k_n。那么，

(i) 当 l 为偶数时，不定方程(2)无解，不定方程(1)的全体正解为

$$x=h_{jl-1}, \quad y=k_{jl-1}, \quad j=1,2,3,\cdots. \tag{3}$$

(ii) 当 l 为奇数时，不定方程(2)的全部正解为

$$x=h_{lj-1}, \quad y=k_{lj-1}, \quad j=1,3,5,\cdots; \tag{4}$$

不定方程(1)的全部正解为

$$x=h_{lj-1}, \quad y=k_{lj-1}, \quad j=2,4,6,\cdots. \tag{5}$$

证　由§3定理8知，若 x, y 是不定方程(1)或(2)的一组正解，那么必有某个 $n\geqslant 0$ 使 $x=h_n, y=k_n$。另一方面由§5式(38)得

$$h_n^2-dk_n^2=(-1)^{n+1}q_{n+1}. \tag{6}$$

由推论9（那里的 $\bar{\xi}_0, \bar{q}_j$ 即这里的 ξ_0, q_j）知，$q_j\neq -1$，及当且仅

当 $l|j$ 时 $q_j=1$。因此，仅当 $n+1=jl(j>0)$ 时，$h_n=h_{lj-1}, k_n=k_{lj-1}$ 才有可能是不定方程(1)或(2)的解，这时

$$h_{lj-1}^2-dk_{lj-1}^2=(-1)^{lj}, \quad j>0.$$

由此就推出所要的全部结论。证毕。

由于当 x,y 是不定方程(1)或(2)的解时，$\pm x, \pm y$(正、负号任意选取）也是不定方程(1)或(2)的解，再注意到 $\pm1, 0$ 是(1)的解，及 $h_{-1}=1, k_{-1}=0$，从定理1立即得到

推论2 在定理1的符号和条件下，

(i) 当 l 为偶数时，不定方程(2)无解，不定方程(1)的全部解为

$$x=\pm h_{lj-1}, \quad y=\pm k_{lj-1}, \quad j=0,1,2,\cdots, \tag{7}$$

其中正、负号任意选取。

(ii) 当 l 为奇数时，不定方程(2)的全部解为

$$x=\pm h_{lj-1}, \quad y=\pm k_{lj-1}, \quad j=1,3,5,\cdots; \tag{8}$$

不定方程(1)的全部解为

$$x=\pm h_{lj-1}, \quad y=\pm k_{lj-1}, \quad j=0,2,4,\cdots, \tag{9}$$

以上正、负号均为任意选取。

定理1表明，为了求出不定方程(1)和(2)的全部正解，就要去求出 $\sqrt{d}$ 的所有渐近分数 $h_{lj-1}/k_{lj-1}(j=1,2,\cdots)$。当然逐个去求不仅麻烦也是不可能的。下面将证明只要求出 h_{l-1}, k_{l-1}，其它的解都可用它很简单地表出。为了叙述和推导方便起见，当 x, y 是不定方程(1)或(2)的(正)解时，我们就说二次无理数 $x+y\sqrt{d}$ 是不定方程(1)或(2)的(正)解。

定理3 设 $\xi_0=\sqrt{d}$，它的循环连分数的周期为 l，渐近分数为 $h_n/k_n(n\geqslant0)$。那么有

$$h_{lj-1}+\sqrt{d}\,k_{lj-1}=(h_{l-1}+\sqrt{d}\,k_{l-1})^j, \quad j=1,2,\cdots. \tag{10}$$

证 记 $\rho_j=h_{lj-1}+\sqrt{d}\,k_{lj-1}$，它的共轭数

$$\rho_j'=h_{lj-1}-\sqrt{d}\,k_{lj-1}.$$

定理1证明了不定方程(1)和(2)(有解的话)的全部正解由 $\rho_j(j\geqslant1)$ 给出。我们有

$$\rho_j\rho'_j=h_{l\,j-1}^2-dk_{l\,j-1}^2=\pm1,\quad j\geqslant1. \tag{11}$$

$$\rho_{j+1}>\rho_j,\quad j\geqslant1. \tag{12}$$

式(12)用到了$\{h_n\}$，$\{k_n\}$均是严格递增数列。由 $\rho_1=h_{l-1}+\sqrt{d}k_{l-1}\geqslant1+\sqrt{d}>1$知，对任意的 $j>1$，必有正整数 k 满足

$$\rho_1^k\leqslant\rho_j<\rho_1^{k+1}.$$

我们来证明必有

$$\rho_j=\rho_1^k. \tag{13}$$

若不然，则有

$$1<\rho_j\rho_1^{-k}<\rho_1. \tag{14}$$

由式(11)知 $\rho_1^{-1}=\pm\rho'_1$，所以

$$\rho_j\rho_1^{-k}=\rho_j(\pm\rho'_1)^k=a+b\sqrt{d},\quad a,b\in\boldsymbol{Z}. \tag{15}$$

由于乘积的共轭数等于共轭数的乘积，利用式(15)得

$$\begin{aligned}a^2-db^2&=(a+b\sqrt{d})(a-b\sqrt{d})\\&=\rho_j(\pm\rho'_1)^k\cdot\rho'_j(\pm\rho_1)^k\\&=\rho_j\rho'_j(\rho_1\rho'_1)^k=\pm1.\end{aligned}$$

由此可推出：$ab\neq0$。因为若 $a=0$ 则上式不可能成立；若$b=0$，则 $a=\pm1$，但由(14)及(15)知，这也不可能。由以上三式得

$$1<a+b\sqrt{d}=\pm1/(a-b\sqrt{d}).$$

显见，a,b 不能均为负。若 a,b 为一正一负，则有

$$|\pm1/(a-b\sqrt{d})|=1/(|a|+\sqrt{d}|b|)\leqslant1/(1+\sqrt{d}),$$

这和上式矛盾。因此，a,b 均为正整数，且 $a+b\sqrt{d}$ 是不定方程(1)或(2)的正解。但由式(12)，(14)及(15)知，

$$a+b\sqrt{d}<\rho_j,\quad j\geqslant1.$$

这和定理 1 矛盾。这就证明了式(13)成立。

显见，为了证明式(10)，只要证明必有$k=j$。下面来证明这一点。由于对任意的$m\geqslant 1$，设$\rho_1^m=a_m+\sqrt{d}\,b_m$，我们有

$$a_m^2-db_m^2=\rho_1^m\cdot(\rho_1^m)'=\rho_1^m\cdot(\rho_1')^m=(\rho_1\rho_1')^m=\pm 1,$$

这里$(\rho_1^m)'$表ρ_1^m的共轭数，所以ρ_1^m $(m\geqslant 1)$一定是不定方程(1)或(2)的正解。由此及定理 1 和式(13)就证明了ρ_1^m $(m\geqslant 1)$和ρ_j $(j\geqslant 1)$一样，都分别给出了不定方程(1)和(2)的全部正解，因此，这两个集合是一样的。注意到（利用式(12)及$\rho_1>1$）

$$\rho_1<\rho_2<\rho_3<\cdots<\rho_j<\cdots,$$

$$\rho_1<\rho_1^2<\rho_1^3<\cdots<\rho_1^j<\cdots,$$

所以式(13)中的$k=j$。证毕。

由定理 3 及推论 2 立即得到（证明留给读者）

推论4 在定理 1 的符号和条件下，

(i) 当l为偶数时，不定方程(2)无解，不定方程(1)的全部解为

$$x+y\sqrt{d}=\pm(h_{l-1}\pm\sqrt{d}\,k_{l-1})^j,\quad j=0,1,2,\cdots,\quad (16)$$

其中正、负号任意选取。

(ii) 当l为奇数时，不定方程(2)的全部解为

$$x+y\sqrt{d}=\pm(h_{l-1}\pm\sqrt{d}\,k_{l-1})^j,\quad j=1,3,5,\cdots;\quad (17)$$

不定方程(1)的全部解为

$$x+y\sqrt{d}=\pm(h_{l-1}\pm\sqrt{d}\,k_{l-1})^j,\quad j=0,2,4,\cdots.\quad (18)$$

以上正、负号均为任意选取。

显见h_{l-1},k_{l-1}是正解中的最小的。如果(2)有解，我们把h_{l-1},k_{l-1}或$h_{l-1}+k_{l-1}\sqrt{d}$称为不定方程(2)的**最小正解**；如果(2)无解，称它为(1)的最小正解。

例 1 求不定方程

$$x^2-73y^2=-1 \tag{19}$$

及

$$x^2-73y^2=1 \tag{20}$$

的全部解。

解 由§5例3知，$\sqrt{73}=\langle 8,\overline{1,1,5,5,1,1,16}\rangle$。周期为7。因此由定理1及定理3知，不定方程(19)的最小正解是 $x=h_6$，$y=k_6$。不难求出

$$h_6/k_6=\langle 8,1,1,5,5,1,1\rangle=1068/125.$$

因此，由推论4知(19)的全部解为

$$x+y\sqrt{73}=\pm(1068\pm125\sqrt{73})^j,$$
$$j=1,3,5,7,\cdots.$$

(20)的全部解为

$$x+y\sqrt{73}=\pm(1068\pm125\sqrt{73})^j,$$
$$j=0,2,4,8,\cdots.$$

例2 求不定方程

$$x^2-8y^2=-1 \tag{21}$$

及

$$x^2-8y^2=1 \tag{22}$$

的全部解。

解 由§3例4知，$\sqrt{8}=\langle 2,\overline{1,4}\rangle$.周期为2。因此由定理1及定理3知，不定方程(21)无解，(22)的最小正解是 $x=h_1,y=k_1$。容易求出

$$h_1/k_1=\langle 2,1\rangle=3/1.$$

所以，由推论4知(22)的全部解为

$$x+y\sqrt{8}=\pm(3\pm\sqrt{8})^j,\quad j=0,1,2,3,\cdots.$$

当 d 比较小或是比较特殊的数时，我们可以不用去求$\sqrt{d}$的循环连分数，而是通过一个一个试算 $y=1,2,\cdots$来求出

$$x^2-dy^2=-1 \text{ 或 } x^2-dy^2=1$$

的最小正解，即第一次找到的一组解。由以上讨论知，当这个第一次找到的解是 $x^2-dy^2=-1$的最小正解时，就可按推论4 (ii)

求出这两个方程的全部解；当是 $x^2-dy^2=1$的最小正解时，$x^2-dy^2=-1$就无解，而按推论 4 (i)就找到 $x^2-dy^2=1$的全部解．例如，在例 2 的情形，取 $y=1$时，$x=3, y=1$就是(22)的解，因而(21)无解。由此立即得到(22)的全部解。下面再举一例。

例 3 求解不定方程

$$x^2-29y^2=-1 \tag{23}$$

及

$$x^2-29y^2=1 \tag{24}$$

的全部解。

解 依次取 $y=1,2,\cdots,12$，由计算知 $\pm1+29y^2$ 均不是完全平方。当 $y=13$时，$-1+29\cdot13^2=70^2$。因此，$x=70, y=13$是不定方程(23)的最小正解。(24)的最小正解，由

$$(70+13\sqrt{29})^2=9801+1820\sqrt{29}$$

知，是 $x=9801, y=1820$。由推论 4 知(23)的全部解是

$$x+y\sqrt{29}=\pm(70\pm13\sqrt{29})^j,\quad j=1,3,5,7,\cdots.$$

(24)的全部解是

$$x+y\sqrt{29}=\pm(70\pm13\sqrt{29})^j,\quad j=0,2,4,6,\cdots.$$

当然，利用$\sqrt{29}=\langle5,\overline{2,1,1,2,10}\rangle$可得到同样结果（留给读者）。

习 题 六

1．利用$\sqrt{d}$的循环连分数来解下面的 Pell 方程。

(i) $x^2-80y^2=-1$，　(ii) $x^2-80y^2=1$，

(iii) $x^2-13y^2=-1$，　(iv) $x^2-13y^2=1$，

(v) $x^2-23y^2=-1$，　(vi) $x^2-23y^2=1$，

(vii) $x^2-28y^2=-1$，　(viii) $x^2-28y^2=1$，

(ix) $x^2-29y^2=-1$，　(x) $x^2-29y^2=1$，

(xi) $x^2-61y^2=-1$，　　(xii) $x^2-61y^2=1$.

2．通过直接试算求最小正解的方法来解下面的 Pell 方程。

(i) $x^2-7y^2=-1$，　　(ii) $x^2-7y^2=1$，

(iii) $x^2-13y^2=-1$，　　(iv) $x^2-13y^2=1$，

(v) $x^2-74y^2=-1$，　　(vi) $x^2-74y^2=1$.

(vii) $x^2-87y^2=-1$，　　(viii) $x^2-87y^2=1$.

3．设 $d>1$ 是非平方数，a 是给定的正整数。证明：$x^2-dy^2=1$有无穷多组解满足 $a|y$。

4．求不定方程 $x^2+(x+1)^2=y^2$ 的全部解，并说明本题的几何意义。

5．证明存在无穷多个正整数 n，使得$1+2+\cdots+n$ 是平方数。

6．设$x_n+y_n\sqrt{2}=(1+\sqrt{2})^n$。证明：

(i) $y_{n+1}=x_n+y_n$，　$x_{n+1}=y_{n+1}+y_n$，　$n\geqslant 1$。

(ii) $y_{2n+1}=y_{n+1}^2+y_n^2$，　$n\geqslant 1$。

(iii) y_{2n+1}^2 是两个相邻自然数的平方和，求出这两个自然数。

(iv) 设 $x_0=1,y_0=0$。当 $n\geqslant m$ 时，

$x_nx_m-2y_ny_m=(-1)^mx_{n-m}$，　$x_ny_m-y_nx_m=(-1)^my_{n-m}$.

(v) $x_{2n+1}=x_{n+1}x_n+2y_{n+1}y_n=2x_{n+1}x_n+(-1)^{n+1}$，

$y_{2n+1}=x_{n+1}y_n+y_{n+1}x_n$.

(vi) $2|y_{2n}$，$2\nmid y_{2n+1}$.

(vii) 当 $n>1$时，x_n 不是完全平方数。

7．设素数 $p\equiv 1 \pmod 4$。证明：$x^2-py^2=-1$必有解。

8．设 $d>1$是非平方数，u,v 是 $x^2-dy^2=1$的最小正解。证明：$x^2-dy^2=-1$有解的充要条件是：

$$s^2+dt^2=u,\quad 2st=v$$

有正整数解 s,t，以及 s,t 是 $x^2-dy^2=-1$的最小正整数解。

以下第9—11题是不用连分数方法直接讨论 Pell 方程。$d>1$

表示非平方数

9．证明：存在无限多对正整数 x,y 满足：$|x^2-dy^2|<1+2\sqrt{d}$（利用 § 4定理8）。

10．证明：一定存在整数 m，使 $x^2-dy^2=m$ 无穷多组解 x_j，y_j，x_j,y_j 是自然数，且对任意的 j_1,j_2 满足：

$$x_{j_1}\equiv x_{j_2}(\mathrm{mod}\ m),\quad y_{j_1}\equiv y_{j_2}(\mathrm{mod}\ m).$$

11．证明：(i) 至少有一组正整数 x,y 满足方程 $x^2-dy^2=1$。设 x_1,y_1 和 x_2,y_2 是两组正整数解，那么 $x_1\leqslant x_2$ 的充要条件是 $y_1\leqslant y_2$。如果正整数解 x_1,y_1 是所有正整数解 x,y 中使 x 为最小的解，那么，x_1,y_1 或 $x_1+\sqrt{d}\,y_1$ 就称为是这方程的最小正解。

(ii) 由 $(x_1+\sqrt{d}\,y_1)^n=x_n+\sqrt{d}\,y_n(n=1,2,\cdots)$ 给出的 x_n，y_n 是 $x^2-dy^2=1$ 的全部正整数解。

12．证明：若 $x^2-dy^2=c$ 有一组解，则必有无穷多组解，这里 $d>1$ 是非平方数，c 为整数。

13．在假定有解的前提下，类似于第12题和第 8 题讨论方程 $x^2-dy^2=\pm4$，其中 $d>1$ 是非平方数。（提示：当 x,y 是解时，考虑 $\rho=(x+y\sqrt{d})/2$，把它看作为解）。

14．设 $d>1$ 是非平方数，c 是整数，$|c|<\sqrt{d}$。若正整数 h,k 是 $x^2-dy^2=c$ 的一组解，且 $(h,k)=1$，那么，h/k 一定是 $\sqrt{d}$ 的渐近分数。

15．设 $d>1$ 是非平方数，ξ,η 是两个正整数，满足 $\xi^2-d\eta^2=1$。证明：若 $\xi>\eta^2/2-1$，则 $\xi+\eta\sqrt{d}$ 是不定方程 $x^2-dy^2=1$ 的最小正解。

第八章　素数分布的初等结果

素数一直是数论中最有趣、最吸引人的研究课题。在前面七章中已经看到对它的性质的研究在数论中的重要作用。除了素数本身的定义之外，实际上所知道的素数性质就是算术基本定理，其它的性质都是从它们推出来的。关于素数有许多有趣的问题。例如，人们一直希望能找到一个表示全体素数的公式，从至今找到的这种"公式"来看，它们都是没有实用和理论价值的，大家都倾向于认为找不到这样一个有用的公式。以 $\pi(x)$ 表示不超过 x 的素数个数。例如：

$$\pi(x)=0, x<2;\quad \pi(5)=3;$$
$$\pi(10.5)=4;\quad \pi(50)=15.$$

寻找一个尽可能简单的 $\pi(x)$ 的表达式很早就吸引了优秀的数学家，但一直没有结果。直到1800年左右，Legendre 和 Gauss 分别提出了以下两个渐近公式：

$$\pi(x)\sim\frac{x}{\ln x-1.08366},\quad x\to+\infty;$$

和（下面的积分在 1 处取主值，称为对数积分）

$$\pi(x)\sim \mathrm{li}\,x=\int_0^x\frac{dt}{\ln t},\quad x\to+\infty.$$

从表 1 可以看出，这两个渐近公式是很精确的。容易看出，$\mathrm{li}\,x\sim x/\ln x, x\to+\infty$。所以，他们实际上都猜测应有

$$\pi(x)\sim x/\ln x,\quad x\to+\infty. \tag{$*$}$$

这就是现在所说的素数定理。这个定理到了1896年才为 J. Hadamard 和 de la Vallée Poussin，利用十分高深的复变函数理论所各

自独立证明。直到1949年，A.Selberg 和 P.Erdös 给出了这个定理的初等证明，但是十分复杂。这些都超出本书的范围①。本章的主要内容就是代替渐近公式(*)，证明 $\pi(x)$的上、下界估计，即著名的 Чебышев 不等式（§2定理1)。

表 1

x	$\pi(x)$	$\frac{x}{\ln x}$	$\mathrm{li}\,x$	$\frac{\pi(x)\ln x}{x}$	$\frac{\pi(x)}{\mathrm{li}\,x}$
1000	168	145	178	1.16	0.95
10000	1229	1086	1246	1.13	0.99
50000	5133	4621	5167	1.11	0.994
100000	9592	8686	9630	1.10	0.996
500000	41538	38103	41606	1.090	0.998
1000000	78498	72382	78628	1.084	0.998
2000000	148933	137849	149055	1.080	0.9992
5000000	348513	324150	348638	1.075	0.9996
10000000	664579	620421	664918	1.071	0.9995

在第一章§2已经介绍了一个具体找出不超过给定正整数N的全体素数的方法，即 Eratosthenes筛法。在§1我们对这方法作进一步更精确的讨论，除了得到对给定的N具体计算 $\pi(N)$的公式外，§1中还对数论中的一个重要的初等方法——筛法——作了最初步的介绍。特别地，引进了十分重要的 Möbius 函数$\mu(n)$。

在本章的最后一节（即§3）中，证明了著名的 Euler 恒等式，它的重要性在于它是算术基本定理的分析等价形式．是用分析方法研究素数理论的基础。

§1 Eratosthenes 筛法

在第一章§2介绍了一个找出不超过给定正整数N的全体素

① 关于素数定理的初等证明可参看：潘承洞和潘承彪合著的《素数定理的初等证明》，上海科学技术出版社，1988.

数的具体方法，只要我们已经知道不超过$\sqrt{N}$的全体素数，这就是古老的 Eratosthenes 筛法。这种方法是十分有效的，至今构造素数表本质上仍是利用这样的办法。现在我们更精确地用公式来表述这一方法。

设$x\geqslant 2$，$\pi(x)$表不超过x的素数个数。以

$$2=p_1<p_2<\cdots<p_s \tag{1}$$

表示所有不超过$\sqrt{x}$的素数，因而$s=\pi(\sqrt{x})$。这样，由第一章§2推论6知：把满足$1\leqslant n\leqslant x$的所有整数n中能被任一$p_i(1\leqslant i\leqslant s)$整除的数去掉后，剩下的就是满足条件

$$\sqrt{x}<p\leqslant x \tag{2}$$

的全部素数p，以及1。所以，剩下的数的个数为

$$T=\pi(x)-\pi(\sqrt{x})+1。\tag{3}$$

我们能不能找到一个公式来表示T呢？在区间$[1,x]$上的正整数n（即满足$1\leqslant n\leqslant x$的正整数n）能被d整除的数的个数是$[[x]/d]=[x/d]$。这样，被取定的p_i整除的数的个数是$[x/p_i]$；被两个取定的不同的p_{i_1},p_{i_2}整除的数的个数是$[x/(p_{i_1}p_{i_2})]$；…；一般的，对取定的$r(1\leqslant r\leqslant s)$，被$r$个取定的两两不同的$p_{i_1},\cdots,p_{i_r}$整除的数的个数是$[x/(p_{i_1}\cdots p_{i_r})]$。如果我们考虑量

$$T_1=[x]-\sum_{i_1=1}^{s}[x/p_{i_1}], \tag{4}$$

则显然有

$$T_1\leqslant T。\tag{5}$$

因为式(4)右边表示依次把区间$[1,x]$上的$[x]$个正整数中能被p_1整除的$[x/p_1]$个整数去掉；被p_2整除的$[x/p_2]$个整数去掉；…；一直到把被p_s整除的$[x/p_s]$个整数去掉之后剩下的整数个数。虽然，那些在$[1,x]$上的恰好只能被一个p_{i_1}整除的整数（即$p_{i_1}^{\alpha_1}$形式的数）在这过程中无重复地每个数被去掉了一次，而对那些在$[1,x]$上的恰好只能被r个（r取定，$2\leqslant r\leqslant s$）两两不同的

$p_{i_1},\cdots,p_{i_r}$整除的整数（即形如$p_{i_1}^{\alpha_1}\cdots p_{i_r}^{\alpha_r}(\alpha_j\geqslant 1)$的数）在这过程中恰好每个数被重复地去掉了 r 次，所以有式(5)成立。那末，如何来弥补这种差异呢？对给定的 $r(1\leqslant r\leqslant s)$，量

$$V_r=\sum_{\substack{i_1=1\\ i_1<i_2<\cdots<i_r}}^{s}\cdots\sum_{i_r=1}^{s}[x/(p_{i_1}\cdots p_{i_r})] \tag{6}$$

是表示对满足以下条件的在$[1,x]$上的正整数 n 的个数的某种有重复的计数：恰好被 r 个两两不同的$p_{i_1},\cdots,p_{i_r}$整除的 n 恰好被计算了一次；恰好被 $t(r<t\leqslant s)$个两两不同的 $p_{i_1},\cdots,p_{i_t}$整除的 n 恰好被重复地计算了$\binom{t}{r}$次（显见对 $t=r$ 这也对）。如果为了弥补 T_1 去掉了过多，而加上 V_2，就要考虑量

$$T_2=T_1+V_2=[x]-V_1+V_2$$

$$=[x]-\sum_{i_1=1}^{s}\left[\frac{x}{p_{i_1}}\right]+\sum_{\substack{i_1=1\\ i_1\neq i_2}}^{s}\sum_{i_2=1}^{s}\left[\frac{x}{p_{i_1}p_{i_2}}\right], \tag{7}$$

这时右边的和式在数量上表示：在区间$[1,x]$上的整数 n 中，把那些恰好被一个 p_{i_1}整除的 n 恰好被去掉了一次；那些恰好被两个不同的 p_{i_1},p_{i_2}整除的 n 去掉了$\binom{2}{1}-\binom{2}{2}=1$次，即也恰好被去掉了一次。但那些恰好被 $t(t>2)$个两两不同的 $p_{i_1},\cdots,p_{i_t}$整除的 n “去掉了”$\binom{t}{1}-\binom{t}{2}$次，由于

$$\binom{t}{1}-\binom{t}{2}=t-(t-1)t/2\leqslant 0,\quad t<2,$$

这表明那些恰好被 $t(>2)$个两两不同的 $p_{i_1},\cdots,p_{i_t}$整除的 n 并

没有被去掉，相反地每个这样的 n 又被以 $\binom{t}{2}-\binom{t}{1}$ 那么多次重复地计算了进去．所以有

$$T_2 \geqslant T. \tag{8}$$

一般的，对给定的 $r(1\leqslant r\leqslant s)$，量

$$U_r = V_1 - V_2 + \cdots + (-1)^{r-1}V_r \tag{9}$$

是表示对满足以下条件的区间 $[1,x]$ 上的整数 n 的个数的某种有"重复"的计数：当 $1\leqslant t\leqslant r$ 时，恰好被 t 个两两不同的 $p_{i_1},\cdots,p_{i_t}$ 整除的 n 在式(9)中恰好被计算了

$$\binom{t}{1}-\binom{t}{2}+\cdots+(-1)^{t-1}\binom{t}{t}=1-(1-1)^t=1\text{次}; \tag{10}$$

而当 $r<t\leqslant s$ 时，恰好被 t 个两两不同的 $p_{i_1},\cdots,p_{i_t}$ 整除的 n 在式(9)中恰好被计算了 $b(t,r)$ 次：

$$b(t,r)=\binom{t}{1}-\binom{t}{2}+\cdots+(-1)^{r-1}\binom{t}{r},$$

$$1\leqslant r<t\leqslant s. \tag{11}$$

由于

$$1=\binom{t}{0}<\binom{t}{1}<\binom{t}{2}<\cdots<\binom{t}{\lfloor t/2\rfloor},\quad t\geqslant 2, \tag{12}$$

所以，当 $r\leqslant t/2$ 时显然有

$$\begin{cases} 1-b(t,r)<0, & 2\nmid r\leqslant t/2, \\ 1-b(t,r)>1, & 2\mid r\leqslant t/2, \end{cases} \quad t\geqslant 2. \tag{13}$$

而当 $r>t/2$ 时（利用式(10)），可得

$$1-b(t,r)=-\sum_{j=r+1}^{t}(-1)^j\binom{t}{j}=-\sum_{j=r+1}^{t}(-1)^j\binom{t}{t-j}$$

$$=(-1)^{t+1}\sum_{j=0}^{t-r-1}(-1)^j\binom{t}{j}$$

$$=(-1)^{t+1}(1-b(t,t-r-1)). \tag{14}$$

由于当 $r>t/2$ 时，$t-r-1<t/2$，由此及式(13)得

$$\begin{cases} 1-b(t,r)<0, & 2\nmid r>t/2,\ r<t, \\ 1-b(t,r)>0 & 2\mid r>t/2,\ r<t, \end{cases}\quad t\geqslant 2. \tag{15}$$

因此综合式（13）及（15）得

$$\begin{cases} b(t,r)>1, & 2\nmid r<t, \\ b(t,r)<1, & 2\mid r<t, \end{cases}\quad t\geqslant 2. \tag{16}$$

记

$$T_r=[x]-U_r,\quad 1\leqslant r\leqslant s. \tag{17}$$

综合以上讨论就证明了

定理1 在式(1),(3),(6),(9)及(17)的条件和符号下，我们有：

(i) U_s 是区间$[1,x]$上与 $p_1\cdots p_s$ 不既约的整数 n 的个数，即满足

$$1\leqslant n\leqslant x,\quad (n,p_1\cdots p_s)>1$$

的 n 的个数；

(ii) T_s 是区间$[1,x]$上与 $p_1\cdots p_s$ 既约的整数 n 的个数，即满足

$$1\leqslant n\leqslant x,\quad (n,p_1\cdots p_s)=1$$

的 n 的个数；

(iii)

$$T=\pi(x)-\pi(\sqrt{x})+1=T_s; \tag{18}$$

(iv)

$$T_{2k-1}<T<T_{2k},\quad 2k<s. \tag{19}$$

式(18)可写为

$$\pi(x)=\pi(\sqrt{x})+T_s-1. \tag{20}$$

这就给出了计算 $\pi(x)$ 的一个公式。例如，取 $x=100$，不超过 $x^{1/2}=10$ 的素数有四个：2,3,5,7，$\pi(10)=4$。我们来计算 U_4。由式(9)和式(6)知，

$$\begin{aligned}U_4&=V_1-V_2+V_3-V_4\\&=\left\{\left[\frac{100}{2}\right]+\left[\frac{100}{3}\right]+\left[\frac{100}{5}\right]+\left[\frac{100}{7}\right]\right\}\\&\quad-\left\{\left[\frac{100}{2\cdot3}\right]+\left[\frac{100}{2\cdot5}\right]+\left[\frac{100}{2\cdot7}\right]+\left[\frac{100}{3\cdot5}\right]\right.\\&\quad\left.+\left[\frac{100}{3\cdot7}\right]+\left[\frac{100}{5\cdot7}\right]\right\}\\&\quad+\left\{\left[\frac{100}{2\cdot3\cdot5}\right]+\left[\frac{100}{2\cdot3\cdot7}\right]+\left[\frac{100}{2\cdot5\cdot7}\right]+\left[\frac{100}{3\cdot5\cdot7}\right]\right\}\\&\quad-\left\{\left[\frac{100}{2\cdot3\cdot5\cdot7}\right]\right\}\\&=117-45+6-0=78.\end{aligned}$$

进而，由式(17)和(20)得到

$$\pi(100)=\pi(10)+100-U_4-1=25.$$

这和第一章§2的结果相符。

事实上，上面的讨论是提出了一个一般方法：对给定的有限整数序列 A，及整数 K，如何去求出序列 A 中所有与 K 既约的整数个数。

定理2 设 A 是一个给定的有限整数序列，K 是给定的正整数，再设 A_d 表示 A 中被正整数 d 整除的所有整数组成的子序列，$p_1,\cdots,p_s$ 是 K 的所有的不同的素因数，以及 $|A_d|$ 表序列 A_d 中的整数个数。那么，序列 A 中所有与 K 既约的数的个数

$$S(A;K)=\sum_{\substack{a\in A\\(a,K)=1}}1$$

$$=|A|-\sum_{r=1}^{s}(-1)^{r}\sum_{\substack{i_1=1\\i_1<i_2<\cdots<i_r}}^{s}\cdots\sum_{i_r=1}^{s}|A_{p_{i_1}\cdots p_{i_r}}|. \tag{21}$$

定理 2 仿照上面讨论的证明留给读者．如果取 A 是由 $1,2,\cdots,[x]$组成的序列，$K=p_1\cdots p_s$，$p_1,\cdots,p_s$ 是不超过 $\sqrt{x}$ 的全部素数，则定理 2 就是定理 1，这时

$$|A_{p_{i_1}\cdots p_{i_r}}|=[x/(p_{i_1}\cdots p_{i_r})].$$

式(21)的表示方式中要利用K的全部素因数，这在推导、表述时都有点不便。下面我们来引进一个十分重要的数论函数，它不仅可以给式(21)一个简洁的表示式，而且用它的性质可以直接、简单地证明定理 2．这就是通常所说的 **Möbius** 函数 $\mu(d)$，变数 d 取正整数值。$\mu(d)$定义为

$$\mu(d)=\begin{cases}1, & d=1;\\(-1)^r, & d=p_1\cdots p_r,\ p_1,\cdots,p_r \text{ 是两两不同的素数；}\\0, & \text{其它，即 } d \text{ 有大于 1 的平方因数。}\end{cases} \tag{22}$$

由定义立即推出，式(21)可改写为

$$S(A;K)=\sum_{\substack{a\in A\\(a,K)=1}}1=\sum_{d|K}\mu(d)|A_d|. \tag{23}$$

我们来证明 Möbius 函数的一个最基本、最重要的性质，由它就可证明定理 2，即式(23)。

引理3 设 n 是正整数，我们有

$$\sum_{d|n}\mu(d)=\left[\frac{1}{n}\right]=\begin{cases}1, & n=1,\\0, & n>1.\end{cases} \tag{24}$$

证 当$n=1$时式(24)显然成立。现设$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$\alpha_j\geqslant 1$。由定义(22)知

$$\sum_{d\mid n}\mu(d)=\sum_{d\mid p_1\cdots p_s}\mu(d)=1-\binom{s}{1}+\binom{s}{2}-\cdots+(-1)^s\binom{s}{s}$$
$$=(1-1)^s=0.$$

这就证明了当$n>1$时式(24)也成立。证毕。

定理2的证明 由引理3知，

$$\sum_{\substack{a\in A\\(a,K)=1}}1=\sum_{a\in A}\sum_{d\mid(a,K)}\mu(d)$$
$$=\sum_{d\mid K}\mu(d)\sum_{\substack{a\in A\\d\mid a}}1=\sum_{d\mid K}\mu(d)\,|A_d|,$$

这就证明了式(23)。也就是式(21)。证毕。

通常我们把式(23)称为Eratosthenes筛法。利用式(23)很容易给出第三章§3式(5)——即$\phi(m)$的计算公式的直接证明。取A为由$1,2,\cdots,m$组成的序列，$K=m$，m由第三章§3式(2)给出，即$m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，$\alpha_j\geqslant 1$。由于

$$|A_d|=m/d,\quad d\mid m,$$

故有

$$\phi(m)=\sum_{\substack{a\in A\\(a,m)=1}}1=\sum_{\substack{a=1\\(a,m)=1}}^{m}1=\sum_{a=1}^{m}\sum_{d\mid(a,m)}\mu(d)$$
$$=\sum_{d\mid m}\mu(d)\sum_{\substack{a=1\\d\mid a}}^{m}1=\sum_{d\mid m}\mu(d)\frac{m}{d}. \tag{25}$$

由定义(22)知

$$\mu(d_1d_2)=\mu(d_1)\mu(d_2),\quad (d_1,d_2)=1, \tag{26}$$

所以有

$$\sum_{d\mid m}\mu(d)/d=\sum_{i_1=0}^{\alpha_1}\cdots\sum_{i_r=0}^{\alpha_r}\mu(p_1^{i_1}\cdots p_r^{i_r})\Big/(p_1^{i_1}\cdots p_r^{i_r})$$

$$= \left\{ \sum_{i_1=0}^{\alpha_1} \mu(p_1^{i_1}) \Big/ p_1^{i_1} \right\} \cdots \left\{ \sum_{i_r=0}^{\alpha_r} \mu(p_r^{i_r}) \Big/ p_r^{i_r} \right\}$$

$$= (1 - 1/p_1) \cdots (1 - 1/p_r), \tag{27}$$

最后一步用了式(22)。由式(25)及(27)就推出第三章 § 3 式(5)。反过来，从式(27)及第三章 § 3 式(5)就推出式(25)。

下面我们利用式(23)来给出 $\pi(x)$ 的上界估计。先证一个引理。

引理4 设 $x \geqslant y \geqslant 2$，$\Phi(x;y)$ 表示不超过 x，且其素因数都大于 y 的所有正整数的个数，那末，

$$x \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) - 2^{\pi(y)} \leqslant 1 + \Phi(x;y) \leqslant x \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) + 2^{\pi(y)}. \tag{28}$$

证 取 A 为序列 $1, 2, \cdots, [x]$，

$$K = P(y) = \prod_{p \leqslant y} p.$$

我们有

$$1 + \Phi(x;y) = S(A;P(y)) = \sum_{\substack{1 \leqslant a \leqslant x \\ (a,P(y))=1}} 1$$

$$= \sum_{d \mid P(y)} \mu(d) \left[\frac{x}{d}\right]$$

$$= x \sum_{d \mid P(y)} \frac{\mu(d)}{d} - \sum_{d \mid P(y)} \mu(d) \left\{\frac{x}{d}\right\}$$

$$= x \prod_{p \leqslant y}\left(1 - \frac{1}{p}\right) - \sum_{d \mid P(y)} \mu(d) \left\{\frac{x}{d}\right\}, \tag{29}$$

最后一步用到了式(27)。由此及下式

$$\left| \sum_{d \mid P(y)} \mu(d) \left\{\frac{x}{d}\right\} \right| \leqslant \sum_{d \mid P(y)} 1 = \tau(P(y)) = 2^{\pi(y)} \tag{30}$$

就推出式(28). 证毕。

定理5 设 $x\geqslant 10$。一定存在正常数 c_1 使得

$$\pi(x)\leqslant c_1 x(\ln\ln x)^{-1}, \tag{31}$$

$$p_n\geqslant c_1^{-1} n\ln\ln n,\quad n\geqslant 5, \tag{32}$$

这里 p_n 表第 n 个素数。

证 容易看出，

$$\pi(x)-\pi(y)\leqslant\Phi(x;y),\quad 2\leqslant y\leqslant x. \tag{33}$$

由此及式(28)得到

$$\pi(x)\leqslant\pi(y)+x\prod_{p\leqslant y}\left(1-\frac{1}{p}\right)+2^{\pi(y)},\quad 2\leqslant y\leqslant x. \tag{34}$$

注意到

$$\prod_{p\leqslant y}\left(1-\frac{1}{p}\right)^{-1}=\prod_{p\leqslant y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)>\sum_{k\leqslant y}\frac{1}{k}$$

$$>\sum_{k\leqslant y}\ln\left(1+\frac{1}{k}\right)=\ln([y]+1)>\ln y, \tag{35}$$

现取 $y=\ln x$，由以上两式得

$$\pi(x)\leqslant x(\ln\ln x)^{-1}+\ln x+2^{\ln x}$$
$$\leqslant x(\ln\ln x)^{-1}+x^{0.7}+\ln x, \tag{36}$$

这就证明式(31)。在式(31)中取 $p_n=x$，注意到 $\pi(p_n)=n$ 及 $p_n>n$，就得到式(32)。这里常数 c_1 的具体数值请读者自己计算。证毕。

素数虽有无穷多个，但由式(31)知，

$$\lim_{x\to+\infty}\frac{\pi(x)}{x}=0, \tag{37}$$

所以，正整数中绝大多数是合数，素数只有很少一部分。

最后，应该指出，本节所讨论的 Eratosthenes 筛法，就是组合数学中的容斥原理在这里的具体应用，熟悉容斥原理的读者，

请自己作比较、分析。

习 题 一

1．求 $\pi(x)$ 的值：$x=200,300,400,500,600,700,800,900,1000$。

2．详细写出仿照§1定理1的证明方法来证明§1定理2的论证。

3．设 n 为任给的正整数，求 $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)$ 的值。

4．求 $\sum_{j=1}^{\infty}\mu(j!)$ 的值。

5．分别求正整数 k 使

$$\mu(k)+\mu(k+1)+\mu(k+2)=0,\pm1,\pm2,\pm3.$$

6．证明：$\sum_{d^2|n}\mu(d)=\mu^2(n)=|\mu(n)|$，这里求和号表示对所有满足 $d^2|n$ 的正整数 d 求和。

7．证明：(i) $\sum_{d|n}\mu^2(d)=2^{\omega(n)}$，$\omega(n)$ 表 n 的不同的素因数的个数，$\omega(1)=0$；

(ii) $\sum_{d|n}\mu(d)\tau(d)=(-1)^{\omega(n)}$.

8．设 k 是给定的正整数．证明：

$$\sum_{d^k|n}\mu(d)=\begin{cases}0, & \text{若存在 } m>1 \text{ 使 } m^k|n;\\ 1 & \text{其它,}\end{cases}$$

这里求和号表示对所有满足 $d^k|n$ 的正整数 d 求和。

9．设 $2|n$．证明：$\sum_{d|n}\mu(d)\phi(d)=0$.

10．设 $f(n)$ 是定义在正整数集合上的函数(称为数论函数)，

再设 $F(n)=\sum_{d\mid n}f(d)$。证明：若对任意的$(n_1,n_2)=1$必有$f(n_1n_2)=f(n_1)f(n_2)$，则对任意的$(n_1,n_2)=1$亦有

$$F(n_1n_2)=F(n_1)F(n_2).$$

11．求 $\sum_{d\mid n}\mu(d)\sigma(d)$的值。

12．(i) 设$k\mid n$，证明：$\sum_{\substack{d=1\\(d,n)=k}}^{n}1=\phi(n/k)$。

(ii) 设$f(n)$是一数论函数，证明：

$$\sum_{d=1}^{n}f((d,n))=\sum_{d\mid n}f(d)\phi(n/d).$$

(iii) 证明：$\sum_{d=1}^{n}(d,n)\mu((d,n))=\mu(n)$。

13．证明：$\mu(n)=\sum_{\substack{d=1\\(d,n)=1}}^{n}e^{2\pi id/n}$。

14．证明：$\sum_{d\leqslant x}\mu(d)\left[\frac{x}{d}\right]=1$。

15．求以下各个$\Phi(x;y)$的值：(i) $x=400$，$y=3,5,7,11$；(ii) $x=1000$，$y=5,7,11,17,29$。并比较$\Phi(x;y)$和$x\prod_{p\leqslant y}\left(1-\frac{1}{p}\right)$的大小（$x,y$取(i),(ii)中的值）。

16．设$k>l\geqslant0$，$(k,l)=1$，及$x>k$。再设A表示整数序列：$1\leqslant a\leqslant x$，$a\equiv l\pmod k$，$\pi(x;k,l)$表示A中的素数个数，以及K表示不超过$\sqrt{x}$且不能整除k的所有素数的乘积。

(i) 证明

$$\pi(x;k,l)=S(A,K)-\varepsilon,$$

这里$S(A,K)$由定理2给出，$\varepsilon=1$当$1\in A$；$\varepsilon=0$当$1\notin A$。

(ii) 利用式(21)求 $\pi(x;4,1)$ 和 $\pi(x;4,3)$. 其中 $x=100$, 300, 500, 700, 1000。

§2 Чебышев 不等式

在第一章§2定理8、第一章§2习题二第30题及上一节的定理5，我们给出了 $\pi(x)$ 及 p_n 的很弱的下界和上界估计。本节将利用第一章§8定理2得到的 $n!$ 的素因数分解式来给出更好的估计，这就是著名的 Чебышев 不等式：

定理1 设 $x\geqslant 2$。我们有

$$\left(\frac{\ln 2}{3}\right)\frac{x}{\ln x}<\pi(x)<(6\ln 2)\frac{x}{\ln x}, \tag{1}$$

及

$$\left(\frac{1}{6\ln 2}\right)n\ln n<p_n<\left(\frac{8}{\ln 2}\right)n\ln n,\quad n\geqslant 2, \tag{2}$$

这里 p_n 是第 n 个素数。

证 先来证明式(1)。设 m 是正整数，

$$M=(2m)!/(m!)^2,$$

由第一章§8例4知，M是正整数①，我们来考虑它的素因数分解式。由第一章§8定理2知（为方便起见，取对数形式）：

$$\begin{aligned}\ln M&=\ln(2m)!-2\ln m!\\&=\sum_{p\leqslant m}\{a(p,2m)-2a(p,m)\}\ln p\\&\quad+\sum_{m<p\leqslant 2m}a(p,2m)\ln p,\end{aligned} \tag{3}$$

这里

$$a(p,n)=\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right]. \tag{4}$$

---

① 当然M就是组合数$\binom{2m}{m}$，由此也可推出M是整数。

显见，

$$\alpha(p,2m)=1,\quad m<p\leqslant 2m. \tag{5}$$

当 $p\leqslant m$ 时，由 $0\leqslant[2y]-2[y]\leqslant 1$ 及式(4)得

$$0\leqslant\alpha(p,2m)-2\alpha(p,m)=\sum_{j=1}^{\infty}\left\{\left[\frac{2m}{p^j}\right]-2\left[\frac{m}{p^j}\right]\right\}$$

$$\leqslant\sum_{p^j\leqslant 2m}1=\left[\frac{\ln(2m)}{\ln p}\right]. \tag{6}$$

这样，由式(3),(5)及(6)得到

$$\sum_{m<p\leqslant 2m}\ln p\leqslant\ln M\leqslant\sum_{p\leqslant 2m}\left[\frac{\ln(2m)}{\ln p}\right]\ln p. \tag{7}$$

因而有

$$\{\pi(2m)-\pi(m)\}\ln m\leqslant\ln M\leqslant\pi(2m)\ln(2m). \tag{8}$$

另一方面，我们直接来估计M的上、下界。我们有

$$M=\frac{2m}{m}\cdot\frac{2m-1}{m-1}\cdots\frac{m+1}{1}\geqslant 2^m, \tag{9}$$

$$M=(2m)!/(m!)^2<(1+1)^{2m}=2^{2m}. \tag{10}$$

由以上三式即得

$$\pi(2m)\ln(2m)\geqslant m\ln 2, \tag{11}$$

$$\{\pi(2m)-\pi(m)\}\ln m<2m\ln 2. \tag{12}$$

当 $x\geqslant 6$ 时，取 $m=[x/2]>2$，这时显然有 $2m\leqslant x<3m$。因而由式（11）得

$$\pi(x)\ln x\geqslant\pi(2m)\ln(2m)>\left(\frac{\ln 2}{3}\right)x,$$

由直接验算知，上式当 $2\leqslant x<6$ 时也成立，这就证明了式（1)的左半不等式。

当 $m=2^k$ 时，由式(12)可得

$$k\{\pi(2^{k+1})-\pi(2^k)\}<2^{k+1},$$

由此及显然估计 $\pi(2^{k+1})\leqslant 2^k\ (k\geqslant 0)$ 可推出

$$(k+1)\pi(2^{k+1})-k\pi(2^k)<3\cdot 2^k.$$

对上式从 $k=0$ 到 $l-1$ 求和，得到

$$l\pi(2^l)<3\cdot 2^l.$$

对任意 $x\geqslant 2$，必有唯一的整数 $h\geqslant 1$，使得 $2^{h-1}<x\leqslant 2^h$，因而有

$$\pi(x)\leqslant\pi(2^h)<3\cdot 2^h/h<(6\ln 2)x/\ln x,$$

这就证明了式(1)的右半不等式。

在上式中取 $x=p_n$，利用 $p_n>n$ 就得到

$$p_n>\left(\frac{1}{6\ln 2}\right)n\ln p_n>\left(\frac{1}{6\ln 2}\right)n\ln n,$$

这就证明了式(2)的左半不等式。设 $n>1$，在式(11)中取 $2m=p_n+1$，得到

$$n\ln(p_n+1)\geqslant(p_n+1)/2\cdot\ln 2.$$

进而有

$$\ln(p_n+1)\leqslant\ln(2n/\ln 2)+\ln\ln(p_n+1). \tag{13}$$

当 $s>-1$ 时，

$$\frac{s}{1+s}\leqslant\ln(1+s)=\int_0^s\frac{dt}{1+t}\leqslant s. \tag{14}$$

取 $s=y/2-1$，由右半不等式即得

$$\ln y\leqslant y/2-(1-\ln 2)<y/2,\quad y>0.$$

取 $y=\ln(p_n+1)$，由上式及式(13)得：

$$\ln(p_n+1)\leqslant 2\ln(2n/\ln 2)<4\ln n,\quad n\geqslant 3.$$

由此及式(13)的前一式，就推出：当 $n\geqslant 3$ 时式(2)的右半不等式成立，当 $n<3$ 时直接验证式(2)的右半不等式成立。证毕。

由定理 1 立即可得到有关素数平均分布的一些估计。为此需要下面的引理。

引理2　设 $y\geqslant 2$，我们有

$$\ln\ln([y]+1)-\ln\ln 2<\sum_{2\leqslant k\leqslant y}\frac{1}{k\ln k}$$

$$<\ln\ln[y]+\frac{1}{2\ln 2}-\ln\ln 2, \tag{15}$$

及

$$[y]\{\ln[y]-1\}+1<\sum_{1\leqslant k\leqslant y}\ln k$$

$$<([y]+1)\{\ln([y]+1)-1\}+2-2\ln 2. \tag{16}$$

证　我们有

$$\int_k^{k+1}\frac{dt}{t\ln t}<\frac{1}{k\ln k}<\int_{k-1}^k\frac{dt}{t\ln t},\quad k\geqslant 3.$$

因此，

$$\sum_{2\leqslant k\leqslant y}\frac{1}{k\ln k}<\frac{1}{2\ln 2}+\int_2^{[y]}\frac{dt}{t\ln t}$$

$$=\ln\ln[y]+\frac{1}{2\ln 2}-\ln\ln 2,$$

$$\sum_{2\leqslant k\leqslant y}\frac{1}{k\ln k}>\int_2^{[y]+1}\frac{dt}{t\ln t}=\ln\ln([y]+1)-\ln\ln 2.$$

由以上两式即得式(15)。类似地，由

$$\int_{k-1}^k\ln t\,dt<\ln k<\int_k^{k+1}\ln t\,dt$$

可得

$$\sum_{1\leqslant k\leqslant y}\ln k<\int_2^{[y]+1}\ln t\,dt=t\ln t\Big|_2^{[y]+1}-\int_2^{[y]+1}dt$$

$$=([y]+1)\ln([y]+1)-([y]+1)+2-2\ln 2,$$

$$\sum_{1<k<y} \ln k > \int_1^{[y]} \ln t\, dt = [y]\ln[y] - [y] + 1.$$

这就证明了式(16)。

由引理 2 及式(2)立即推出

定理3 设 $x \geqslant 5$。一定存在正常数 $c_1, c_2, \cdots, c_6$，使得

$$c_1 \ln\ln x < \sum_{p<x} \frac{1}{p} < c_2 \ln\ln x①, \tag{17}$$

$$c_3 x < \sum_{p<x} \ln p < c_4 x, \tag{18}$$

$$c_5 \ln x < \sum_{p<x} \frac{\ln p}{p} < c_6 \ln x. \tag{19}$$

此外，

$$\lim_{n\to\infty} (\ln p_n)/(\ln n) = 1. \tag{20}$$

证 式(20)由式(2)立即推出。由式(2)容易推出

$$a_1 \ln n < \ln p_n < a_2 \ln n, \quad n \geqslant 2, \tag{21}$$

$$a_3 \ln\ln n < \ln\ln p_n < a_4 \ln\ln n, \quad n \geqslant 25, \tag{22}$$

a_1, a_2, a_3, a_4 是和 n 无关的正常数。下面来证式(17)—(19).显见，不妨设 $x \geqslant 100$。令 $p_m \leqslant x < p_{m+1}$，所以 $m \geqslant 25$.先来证式(17)。由式(2)知，存在正常数 a_5, a_6 使得

$$a_5 \sum_{k=2}^{m} \frac{1}{k\ln k} < \sum_{p<x} \frac{1}{p} = \sum_{k=1}^{m} \frac{1}{p_k} < a_6 \sum_{k=2}^{m} \frac{1}{k\ln k} + \frac{1}{2}.$$

进而由式(15)，$m \geqslant 25$ 推出：存在正常数 a_7, a_8 使得

$$a_7 \ln\ln(m+1) < \sum_{p<x} \frac{1}{p} < a_8 \ln\ln m,$$

进而由式(22)及 $m \geqslant 25$ 知，

$$\ln\ln m < a_3^{-1} \ln\ln p_m \leqslant a_3^{-1} \ln\ln x,$$

① 请比较式（17）的左半不等式和第一章习题二第29题（ii）。

$$\ln\ln(m+1) > a_4^{-1}\ln\ln p_{m+1} > \ln\ln x.$$

由以上三式就推出式(17)。

下面来证式(18)。由式(21)得

$$a_1\sum_{k=2}^{m}\ln k < \sum_{p\leqslant x}\ln p = \sum_{k=1}^{m}\ln p_m < a_2\sum_{k=2}^{m}\ln k + \ln 2.$$

利用式(16)及 $m\geqslant 25$，由此就推出：存在正常数 a_9、a_{10} 使得

$$a_9(m+1)\ln(m+1) < \sum_{p\leqslant x}\ln p < a_{10}m\ln m.$$

进而由式(2)及 $m\geqslant 25$ 推出：

$$m\ln m < (6\ln 2)p_m \leqslant (6\ln 2)x,$$

及

$$(m+1)\ln(m+1) > (\ln 2/8)p_{m+1} > (\ln 2/8)x.$$

由以上三式就推出式(18)。

最后来证式(19)。由式(2)及(21)知，存在正常数 a_{11}, a_{12} 使得

$$a_{11}/n < (\ln p_n)/p_n < a_{12}/n,\quad n\geqslant 1.$$

因此

$$a_{11}\sum_{k=1}^{m}\frac{1}{k} < \sum_{p\leqslant x}\frac{\ln p}{p} = \sum_{k=1}^{m}\frac{\ln p_k}{p_k} < a_{12}\sum_{k=1}^{m}\frac{1}{k}.$$

由此及

$$\ln(m+1) = \int_1^{m+1} t^{-1}\mathrm{d}t < \sum_{k=1}^{m}\frac{1}{k} < 1 + \int_1^{m} t^{-1}\mathrm{d}t = 1 + \ln m$$

得到

$$a_{11}\ln(m+1) < \sum_{p\leqslant x}(\ln p)/p < 2a_{12}\ln m.$$

由式(21)可得

$$\ln m < a_1^{-1}\ln p_m < a_1^{-1}\ln x,$$

$$\ln(m+1) > a_2^{-1}\ln p_{m+1} > a_2^{-1}\ln x.$$

由以上三式就推出式(19)。证毕。

关于素数有一个很出名的猜测：对每个整数 $m>1$，必有素数 p 满足 $m<p\leqslant 2m$，即

$$\pi(2m)-\pi(m)\geqslant 1,\quad m\geqslant 1. \tag{23}$$

通常称这为Betrand假设。从式(1)还不能立即推出式(23)。从式(3)和(5)知：

$$\sum_{m<p\leqslant 2m}\ln p=\ln M-\sum_{p\leqslant m}\{a(p,2m)-2a(p,m)\}\ln p. \tag{24}$$

如果能更精确估计上式右边的两项，证明右边当 $m\geqslant 1$ 时一定大于零，则就证明了式(23)。这就是下面定理4证明的途径。

定理4 当 $m\geqslant 1$ 时，式(23)一定成立，即必有一个素数 p 满足 $m<p\leqslant 2m$。

证 我们先来更精确计算 $a(p,2m)-2a(p,m)$ 的值。当 $m\geqslant 5$ 时，我们有

$$p^2>4m^2/9>2m,\quad 当\ 2m/3<p\leqslant m,$$

所以，当 $2m/3<p\leqslant m$ 时有

$$a(p,2m)-2a(p,m)=[2m/p]-2[m/p]=0;$$

另外，由式(6)知，

$$a(p,2m)-2a(p,m)\leqslant\left[\frac{\ln 2m}{\ln p}\right]<2,\quad 当\sqrt{2m}<p\leqslant 2m/3.$$

由此及式(6)，从式(24)推出：当 $m\geqslant 5$ 时有

$$\begin{aligned}\sum_{m<p\leqslant 2m}\ln p&\geqslant\ln M-\sum_{\sqrt{2m}<p\leqslant 2m/3}\ln p\\&\quad-\sum_{p\leqslant\sqrt{2m}}\{a(p,2m)-2a(p,m)\}\ln p\\&\geqslant\ln M-\sum_{\sqrt{2m}<p\leqslant 2m/3}\ln p\\&\quad-\pi(\sqrt{2m})\ln(2m).\end{aligned}\tag{25}$$

式(25)改进了式(7)和式(8)的右半不等式。下面我们要更精确地估计式(25)的右边三项。

首先，由$\binom{2m}{m}\geqslant\binom{2m}{k}$，$1\leqslant k\leqslant 2m-1$，及$\binom{2m}{m}\geqslant 2$得

$$(1+1)^{2m}=2+\binom{2m}{1}+\cdots+\binom{2m}{2m-1}\leqslant 2m\binom{2m}{m}.$$

因而有

$$M=\binom{2m}{m}\geqslant 2^{2m}/(2m), \tag{26}$$

这改进了式(9)。其次，当 $y\geqslant 16$ 时，不超过 y 的奇合数的个数至少有 9，15 两个，而 $\pi(y)$ 等于不超过 y 的奇数个数与不超过 y 的奇合数个数之差(为什么)，所以

$$\pi(y)\leqslant(y+1)/2-2<y/2-1,\quad y\geqslant 16.$$

因而有

$$\pi(\sqrt{2m})<\sqrt{m/2}-1,\quad m\geqslant 128. \tag{27}$$

最后，为了估计式(25)右边的第二项，需要下边的引理。

引理 5[①] 设 $x\geqslant 2$。我们有

$$\sum_{p\leqslant x}\ln p<(2\ln 2)x. \tag{28}$$

证 显见，只要考虑 x 是整数的情形。用归纳法来证。当 $x=2$ 时式(28)显然成立，假设式(28)对所有的 $x<k$ $(k\geqslant 3)$ 成立。若 k 是合数，则当 $x=k$ 时式(28)显然成立；若 k 是素数，设 $k=2n+1$ $(n\geqslant 1)$。由归纳假设知

$$\sum_{p\leqslant n+1}\ln p<(2\ln 2)(n+1). \tag{29}$$

利用

---

① 这引理定出了式(18)中的较好的正常数 c_1。

$$\prod_{n+2\leqslant p\leqslant 2n+1} p \Big| \frac{(2n+1)!}{n!(n+1)!} = \binom{2n+1}{n},$$

及

$$(1+1)^{2n+1} > \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n},$$

就推出

$$\sum_{n+2\leqslant p\leqslant 2n+1} \ln p < (2\ln 2)n.$$

由此及式(29)就证明了式(28)当 $x=k=2n+1$ 为素数时也成立。因此，式(28)对一切 $x\geqslant 2$ 都成立。证毕。

由式(28)可得

$$\sum_{\sqrt{2m}<p\leqslant 2m/3} \ln p < ((4\ln 2)/3)m.$$

综合式(25)，(26)，(27)及上式即得：当 $m\geqslant 128$ 时，

$$\begin{aligned}\sum_{m<p\leqslant 2m} \ln p &> 2m\ln 2 - \ln(2m) \\ &\quad - ((4\ln 2)/3)m - (\sqrt{m/2}-1)\ln(2m) \\ &= m((2\ln 2)/3 - 2(\ln\sqrt{2m})/\sqrt{2m}).\end{aligned} \qquad (30)$$

由于

$$(y^{-1}\ln y)' = (1-\ln y)/y^2,$$

所以当 $y\geqslant e$ 时，函数 $y^{-1}\ln y$ 递减，因而

$$y^{-1}\ln y \leqslant (\ln 2)/4, \quad y\geqslant 16.$$

由此及式(30)得到

$$\sum_{m<p\leqslant 2m} \ln p > ((\ln 2)/6)m, \quad m\geqslant 128. \qquad (31)$$

这就证明了当 $m\geqslant 128$ 时定理成立。当 $m<128$ 可直接验证存在素数 p 满足 $m<p\leqslant 2m$：

$$m=1,\ p=2; \qquad m=2,\ p=3; \qquad m=3,\ p=5;$$

$$4\leqslant m\leqslant 6,\ p=7;\qquad 7\leqslant m\leqslant 12,\ p=13;$$
$$13\leqslant m\leqslant 22,\ p=23;\qquad 23\leqslant m\leqslant 42,\ p=43;$$
$$43\leqslant m\leqslant 82,\ p=83;\qquad 83< m\leqslant 127,\ p=131.$$

证毕。

为了证明素数定理，Чебышев 引进了两个重要函数来代替 $\pi(x)$，它们是

$$\theta(x)=\sum_{p\leqslant x}\ln p,\tag{32}$$

和

$$\psi(x)=\sum_{n\leqslant x}\Lambda(n),\tag{33}$$

其中 $\Lambda(n)$ 是定义为

$$\Lambda(n)=\begin{cases}\ln p, & n=p^{\alpha},\ p\text{ 素数},\ \alpha\geqslant 1,\\ 0, & \text{其它},\end{cases}\tag{34}$$

通常称 $\Lambda(n)$ 为 Mangoldt 函数。这两个函数讨论起来要比 $\pi(x)$ 方便得多。从上面的讨论可以看出为什么要引进 $\theta(x)$ 的理由，引进 $\psi(x)$ 的理由将在下节说明。我们先来证明一个定理说明这三个函数之间的关系。

定理6 设 $x\geqslant 2$。那么，存在正常数 c_7 使得

$$(\ln x-c_7)\pi(x)<\theta(x)<(\ln x)\pi(x),\tag{35}$$

及

$$\theta(x)\leqslant\psi(x)\leqslant\theta(x)+x^{1/2}\ln x.\tag{36}$$

证 先来证式(35)。我们有

$$\theta(x)=\sum_{p\leqslant x}\ln p=\sum_{k\leqslant x}\ln k(\pi(k)-\pi(k-1))$$

$$=-\sum_{k=2}^{[x]-1}\pi(k)(\ln(k+1)-\ln k)+\pi([x])\ln[x].$$

利用式(14)可得

$$\frac{1}{y+1}<-\ln\left(1-\frac{1}{y+1}\right)=\ln\left(1+\frac{1}{y}\right)<\frac{1}{y},\quad y\geqslant 1,\qquad (37)$$

由此得到

$$\pi(x)\ln[x]-\sum_{k=2}^{[x]-1}\frac{\pi(k)}{k}<\theta(x)<\pi(x)\ln x-\sum_{k=2}^{[x]-1}\frac{\pi(k)}{k+1}.$$

由式(1)得

$$\sum_{k=2}^{[x]-1}\frac{\pi(k)}{k}<a_1\sum_{k=2}^{[x]-1}\frac{1}{\ln k}<\frac{a_1}{\ln 2}+a_1\int_2^x\frac{dt}{\ln t}$$

$$=\frac{a_1}{\ln 2}+a_1\left\{\int_2^{\sqrt{x}}\frac{dt}{\ln t}+\int_{\sqrt{x}}^x\frac{dt}{\ln t}\right\}$$

$$<\frac{a_1}{\ln 2}+\frac{a_1}{\ln 2}\sqrt{x}+2a_1\frac{x}{\ln x}$$

$$<a_2\pi(x),$$

最后一步用到了由式(14)的后一式推出的$\sqrt{x}<x/\ln x$（为什么），以及式(1)，这里的a_1,a_2是正常数．此外，

$$\ln[x]>\ln(x-1)=\ln x+\ln(1-1/x)$$
$$>\ln x-1/(x-1),$$

最后一步用到了式(37)．由以上三式即得式(35)．

下面来证式(36)．由式(34)知

$$\psi(x)=\sum_{n\leqslant x}\Lambda(n)=\sum_{p^a\leqslant x}\ln p,$$

右边是对素变数p，及整变数a满足条件$p^a\leqslant x$的范围上求和．显见，对固定的p，a的求和范围是$1\leqslant a\leqslant(\ln x)/\ln p$，所以有（记$a_p=(\ln x)/\ln p$）

$$\psi(x)=\sum_{p\leqslant x}\ln p+\sum_{p^a\leqslant x,\ a\geqslant 2}\ln p$$

$$= \theta(x) + \sum_{p \leqslant \sqrt{x}} \ln p \sum_{2 \leqslant a \leqslant a_p} 1$$

$$\leqslant \theta(x) + \sum_{p \leqslant \sqrt{x}} \ln p \cdot \ln x / \ln p$$

$$\leqslant \theta(x) + x^{1/2} \ln x.$$

由此就推出式(36)。证毕。

定理 6 就表明为什么可以用 $\theta(x)$ 或 $\psi(x)$ 来代替 $\pi(x)$ 研究素数分布，具体的说有下面的

定理 7　设 $x \geqslant 2$。(i) 以下三个命题等价：

(a) 存在正常数 d_1, d_2 使得

$$d_1 x / \ln x < \pi(x) < d_2 x / \ln x.$$

(b) 存在正常数 d_3, d_4 使得

$$d_3 x < \theta(x) < d_4 x.$$

(c) 存在正常数 d_5, d_6 使得

$$d_5 x < \psi(x) < d_6 x;$$

(ii) 以下三个命题等价：

(d) $\lim\limits_{x \to \infty} \pi(x) \ln x / x = 1$.

(e) $\lim\limits_{x \to \infty} \theta(x) / x = 1$.　　(f) $\lim\limits_{x \to \infty} \psi(x) / x = 1$.

这两个结论容易从定理 6 推出，详细推导留给读者。下面我们来直接证明定理 7 的(c)，由此利用等价性就推出式(1)（当然常数可以不同），而这里的推导要简洁些。为此，先证几个引理。

引理 8　设整数 $n \geqslant 1$。我们有

$$\sum_{d \mid n} \Lambda(d) = \ln n. \tag{38}$$

证　$n = 1$ 显然成立。若 $n > 1$，设 n 的素因数分解式是：

$$n = p_1^{a_1} \cdots p_r^{a_r}.$$

由 $\Lambda(d)$ 的定义(式(34))知，

$$\sum_{d\mid n}\Lambda(d)=\sum_{d\mid p_1^{\alpha_1}}\Lambda(d)+\cdots+\sum_{d\mid p_r^{\alpha_r}}\Lambda(d)$$

$$=\alpha_1\ln p_1+\cdots+\alpha_r\ln p_r=\ln n.$$

这就证明了式(38)。这个性质是算术基本定理的推论。

引理 9　设$x\geqslant 1$。我们有

$$\sum_{m\leqslant x}\psi(x/m)=\ln([x]!).\tag{39}$$

证　由$\psi(x)$的定义(式(33))知，

$$\sum_{m\leqslant x}\psi(x/m)=\sum_{m\leqslant x}\sum_{k\leqslant x/m}\Lambda(k)$$

$$=\sum_{m\leqslant x}\sum_{km\leqslant x}\Lambda(k),\tag{40}$$

作整变数替换$km=d$，$k=k$，上式变为

$$\sum_{m\leqslant x}\psi(x/m)=\sum_{d\leqslant x}\sum_{k\mid d}\Lambda(k)=\sum_{d\leqslant x}\ln d,$$

最后一步用到了式(38)。由此就推出式(39)。

应该指出，式(39)是$n!$的素因数分解式——第一章§8定理2——的等价形式。先来证明从式(39)可推出$n!$的素因数分解式。由式(40)可得：

$$\sum_{m\leqslant x}\psi(x/m)=\sum_{k\leqslant x}\Lambda(k)\sum_{m\leqslant x/k}1$$

$$=\sum_{k\leqslant x}\left[\frac{x}{k}\right]\Lambda(k).\tag{41}$$

由$\Lambda(d)$的定义得

$$\sum_{k\leqslant x}\left[\frac{x}{k}\right]\Lambda(k)=\sum_{p^\alpha\leqslant x,\ \alpha\geqslant 1}\left[\frac{x}{p^\alpha}\right]\ln p$$

$$=\sum_{p\leqslant x}\ln p\sum_{\alpha=1}^{\infty}\left[\frac{x}{p^\alpha}\right].\tag{42}$$

在式(39)中取 $x=n$，利用以上两式即得

$$\ln(n!)=\sum_{p\leq n}\ln p\sum_{a=1}^{\infty}\left[\frac{n}{p^a}\right],\tag{43}$$

这就是$n!$的素因数分解式(取对数形式)。反过来，从式(43)成立可推出式(39)。这只要在式(43)中取 $n=[x]$，注意到$[[x]/p^a]=[x/p^a]$，由式(43)（$n=[x]$），(42)及(41)就推出式(39)。这是给出了引理 9 的一个新的证明(但它的基础仍是算术基本定理)，由这一证明也可看出引入函数 $\psi(x)$的道理。

现在，我们来证明定理 7 的(c)。

定理10 设$x\geqslant2$。我们有

$$(1/4)(\ln2)x<\psi(x)<(4\ln2)x.\tag{44}$$

证 设 m 为正整数。由式(39)得

$$\begin{aligned}\ln(2m)!-2\ln m! &= \sum_{k\leq 2m}\psi(2m/k)-2\sum_{d\leq m}\psi(m/d)\\ &=\sum_{k\leq 2m}\psi(2m/k)-2\sum_{d\leq m}\psi(2m/(2d))\\ &=\sum_{k\leq 2m}(-1)^{k-1}\psi(2m/k).\end{aligned}\tag{45}$$

因而有

$$\psi(2m)-\psi(m)\leqslant\ln\frac{(2m)!}{(m!)^2}\leqslant\psi(2m).\tag{46}$$

由此及式(9)，式(10)推出

$$\psi(2m)\geqslant m\ln2,\tag{47}$$

$$\psi(2m)-\psi(m)\leqslant 2m\ln2.\tag{48}$$

当 $x\geqslant2$ 时，由式(47)得

$$\psi(x)\geqslant\psi(2[x/2])\geqslant[x/2]\ln2>(1/4)(\ln2)x,$$

这就证明了式(44)的左半不等式。而对 $x\geqslant2$ 必有唯一的正整数 n 满足 $2^{m-1}<x\leqslant2^m$。这样，由式(48)得

$$\psi(x)\leqslant\psi(2^m)=\sum_{k=0}^{m-1}\{\psi(2^{k+1})-\psi(2^k)\}$$

$$\leqslant\sum_{k=0}^{m-1}2^{k+1}\ln2<2^{m+1}\ln2$$

$$<(4\ln2)x,$$

这就证明了式(44)右边的不等式．证毕。

习 题 二

1．设 $\pi_2(x)$ 表示所有不超过 x 且恰为两个素数乘积的正整数的个数。证明：存在正常数 c_1,c_2，使得

$$c_1\frac{x\ln\ln x}{\ln x}<\pi_2(x)<c_2\frac{x\ln\ln x}{\ln x},\quad x\geqslant4.$$

2．证明：当 $m\geqslant6$ 时，必有两个素数 p,q 满足 $m<p<q<2m$。

3．证明：存在正常数 c 使得

$$\pi(2x)-\pi(x)>cx/\ln x,\quad x\geqslant2.$$

4．证明：(i) $\psi(x)=\sum_{n=1}^{\infty}\theta(x^{1/n})$.

(ii) $\theta(x)=\sum_{n=1}^{\infty}\mu(n)\psi(x^{1/n})$.

5．证明：存在正常数 c，使得

$$\psi(x)<\theta(x)+cx^{1/2}.$$

6．证明：素数定理 $\lim\limits_{x\to\infty}\pi(x)(\ln x)/x=1$ 等价于 $\lim\limits_{n\to\infty}p_n/(n\ln n)=1$，这里 p_n 表示第 n 个素数。

7．设 $T(x)=\ln([x]!)$。证明：当 $x\geqslant1$ 时

$$\psi(x)=\sum_{n\leqslant x}\mu(n)T(x/n).$$

8．设$T(x)$同上题，及$U(x)=T(x)-T(x/2)-T(x/3)-T(x/5)+T(x/30)$。证明：

(i) $U(x)=Ax+5\theta_1(\ln x+1)$，其中$|\theta_1|\leqslant 1$，

$$A=(7/15)\ln 2+(3/10)\ln 3+(1/6)\ln 5=0.92129\cdots;$$

(ii) $U(x)=\sum_{j=1}^{\infty}a_j\psi(x/j)$，$a_{j+30}=a_j, j\geqslant 1$，并具体定出$a_j$；

(iii) $\psi(x)\geqslant U(x)\geqslant\psi(x)-\psi(x/6)$；

(iv) 当$x\geqslant 1$时，

$$Ax-5(\ln x+1)\leqslant\psi(x)\leqslant(6A/5)x+(3\ln x+5)(\ln x+1).$$

9．证明：存在正常数A_1, A_2，使得

(i) $\sum_{k\leqslant x}\Lambda(k)/k=\ln x+\Delta_1(x)$，$|\Delta_1(x)|\leqslant A_1$，$x\geqslant 1$；

(ii) $\sum_{p\leqslant x}(\ln p)/p=\ln x+\Delta_2(x)$，$|\Delta_2(x)|\leqslant A_2$，$x\geqslant 2$。

10．设$f(x)$是区间$[a,b]$上的非负递增函数。证明

$$\left|\sum_{a<n\leqslant b}f(n)-\int_a^b f(t)\mathrm{d}t\right|\leqslant f(b).$$

11．设$f(x)$是区间$[a,b]$上的非负递减函数。证明

$$\left|\sum_{a<n\leqslant b}f(n)-\int_a^b f(t)\mathrm{d}t\right|\leqslant f(a).$$

12．利用第12,13题来估计引理2中两个和式的上、下界。

13．证明：无穷级数$\sum_p(\ln\ln p)^{-\lambda}p^{-1}$，当$\lambda>1$时收敛，当$\lambda\leqslant 1$时发散。

14．利用$\Lambda(n)=\sum_{d\mid n}\Lambda(d)\left\{\sum_{l\mid n/d}\mu(l)\right\}$，证明：

$$\Lambda(n)=\sum_{l\mid n}\mu(l)\ln(n/l)=-\sum_{l\mid n}\mu(l)\ln l.$$

进而推出第 7 题。

15．设 $f(n)$ 是正整数变数的函数，$F(n)=\sum_{d\mid n}f(d)$。利用

$$f(n)=\sum_{d\mid n}f(d)\left\{\sum_{l\mid n/d}\mu(l)\right\},$$

证明：$f(n)=\sum_{d\mid n}\mu(d)F(n/d)$。反过来，若先给定正整数变数函数 $F(n)$，及设 $f(n)=\sum_{d\mid n}\mu(d)F(n/d)$。证明：$F(n)=\sum_{d\mid n}f(d)$。这一对关系式通常称为 Möbius 反转公式。

§3* Euler 恒等式

关于正整数与素数之间的关系，我们证明了两个重要结论。一个是算术基本定理，它是最基本的；另一个是由它推出的 $n!$ 的素因数分解式，它的等价形式是 §2 式(39)。本节要来证明算术基本定理的一个分析等价形式，这一思想在第一章 §2 习题二第28题给出的素数有无穷多个的另一证明中已经用到。先来证明几个引理。

引理 1 当实数 $s>1$ 时，无穷乘积

$$\prod_{p}\left(1-\frac{1}{p^{s}}\right)^{-1}\tag{1}$$

收敛且大于 1，这里的连乘号表示对所有素数求积。

证 由 §2 式(14)可得：

$$0<\frac{1}{p^{s}}<\ln\left(1-\frac{1}{p^{s}}\right)^{-1}=\ln\left(1+\frac{1}{p^{s}-1}\right)<\frac{1}{p^{s}-1},\quad s>0.\tag{2}$$

因而有

$$\sum_p \frac{1}{p^s} < \sum_p \ln\left(1-\frac{1}{p^s}\right)^{-1} < \sum_p \frac{1}{p^s-1}$$

$$< 2\sum_p \frac{1}{p^s} < 2\sum_{n=1}^{\infty}\frac{1}{n^s}, \quad s>1, \tag{3}$$

这里求和号 $\sum\limits_p$ 表示对全体素数 p 求和。由于当 $s>1$ 时，级数 $\sum\limits_{n=1}^{\infty} n^{-s}$ 收敛，所以由式(3)知正项级数

$$\sum_p \ln\left(1-\frac{1}{p^s}\right)^{-1}$$

当 $s>1$ 时也收敛，由此就推出无穷乘积(1)收敛，它的值大于 1 是显然的。证毕。

假定我们还没有证明算术基本定理，当 $n>1$ 时由第一章 §2 定理 5 知 n 必可表为

$$n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}. \tag{4}$$

由于必有 $p_j^{\alpha_j} \leqslant n$，所以这种表法的个数是有限的，设不计次序的这种表法个数为 $c(n)$，显然有 $c(n)\geqslant 1$。我们约定 $c(1)=1$。

引理 2　当实数 $s>1$ 时，

$$\prod_p\left(1-\frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty}\frac{c(n)}{n^s}. \tag{5}$$

证　当 $s>1$ 时，

$$\left(1-\frac{1}{p^s}\right)^{-1} = 1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots.$$

对任给的正整数 N，取正整数 k，$2^{k-1}\leqslant N<2^k$，我们有

$$\sum_{n=1}^{N}\frac{c(n)}{n^s} \leqslant \prod_{p\leqslant N}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots+\frac{1}{p^{ks}}\right)$$

$$\leqslant\prod_{p<N}\left(1-\frac{1}{p^s}\right)^{-1}\leqslant\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1},\quad s>1. \tag{6}$$

当 $s>1$ 时由引理 1 知上式的无穷乘积收敛，所以由上式知式(5)右边的正项级数收敛，且有

$$\sum_{n=1}^{\infty}\frac{c(n)}{n^s}\leqslant\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}. \tag{7}$$

反过来，对任给的正整数 M 及 h，取

$$N_1=\prod_{p\leqslant M}p^h,$$

这里的连乘号表示对所有不超过 M 的素数求积。由 $c(n)$ 的定义知

$$\prod_{p<M}\left(1+\frac{1}{p^s}+\cdots+\frac{1}{p^{hs}}\right)\leqslant\sum_{n=1}^{N_1}\frac{c(n)}{n^s}<\sum_{n=1}^{\infty}\frac{c(n)}{n^s},\quad s>1.$$

最后一步用到了已经证明的正项级数 $\sum\limits_{n=1}^{\infty}\frac{c(n)}{n^s}$ 的收敛性。令 $h\to+\infty$，由上式得

$$\prod_{p<M}\left(1-\frac{1}{p^s}\right)^{-1}\leqslant\sum_{n=1}^{\infty}\frac{c(n)}{n^s},\quad s>1.$$

再令 $M\to+\infty$，由上式得

$$\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}\leqslant\sum_{n=1}^{\infty}\frac{c(n)}{n^s},\quad s>1.$$

由此及式(7)就证明了所要的结论。

定理 3 算术基本定理，即

$$c(n)=1,\quad n\geqslant 1, \tag{8}$$

等价于

$$\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s>1. \tag{9}$$

证 利用引理 2，从式(8)成立就推出式(9)成立。反过来，

若式(9)成立，则由引理 2 知

$$\sum_{n=1}^{\infty}\frac{c(n)-1}{n^s}=0,\quad s>1.$$

由于对所有的 n 都有 $c(n)-1\geqslant 0$，由此及上式就推出式(8)成立(为什么)。证毕。

应该指出的是，就我们所知至今还没有不利用算术基本定理来推出式(9)的直接证明。式(9)通常称为 Euler 恒等式，式(9)右边的级数通常记作

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s>1, \tag{10}$$

称为 Riemann ζ 函数。关系式(9)的重要性在于它是应用分析方法研究素数性质的基础。这些当然完全超出了本书讨论的范围。利用本节的方法和关系式(9)可以得到许多有趣而重要的关系式，这些将安排在习题中。

习 题 三

1．设 $f(n)$ 是定义在正整数集合上的函数，s 是实数，级数 $\sum_{n=1}^{\infty}f(n)n^{-s}$① 绝对收敛且不等于零。证明：

(i) 若当 $(m,n)=1$ 时 $f(mn)=f(m)f(n)$，则

$$\sum_{n=1}^{\infty}f(n)n^{-s}=\prod_{p}(1+f(p)p^{-s}+f(p^2)p^{-2s}+\cdots);$$

(ii) 若对任意的 m,n 有 $f(mn)=f(m)f(n)$，则

$$\sum_{n=1}^{\infty}f(n)n^{-s}=\prod_{p}(1-f(p)p^{-s})^{-1},$$

这里右边的两个无穷乘积都绝对收敛。

① 这种形式的级数称为Dirichlet级数。

2．设 s 是实数．级数 $\sum_{n=1}^{\infty} f(n)n^{-s}$ 和 $\sum_{m=1}^{\infty} g(m)m^{-s}$ 都绝对收敛。证明：

$$\sum_{n=1}^{\infty} f(n)n^{-s} \cdot \sum_{m=1}^{\infty} g(m)m^{-s} = \sum_{l=1}^{\infty} h(l)l^{-s},$$

这里

$$h(l) = \sum_{n \mid l} f(n)g(l/n) = \sum_{n \mid l} f(l/n)g(n)$$

$$= \sum_{nm=l} f(n)g(m),$$

且右边的无穷级数也绝对收敛。

3．证明：(i) $\sum_{n=1}^{\infty} \mu(n)n^{-s} = \prod_{p}(1-p^{-s})$，$s>1$；

(ii) $\sum_{n=1}^{\infty} \mu(n)n^{-s} = 1/\zeta(s)$，$s>1$；

(iii) 由(ii) 给出§1 引理 3 的另一证明。

4．证明：当$s>1$时，$\sum_{n=1}^{\infty} \mu^2(n)n^{-s} = \zeta(s)/\zeta(2s)$。

5．设 $\Omega(n)$表 n 的不同的素因子个数，$\Omega(1)=0$，及 $\lambda(n) = (-1)^{\Omega(n)}$。证明：

(i) $\sum_{n=1}^{\infty} \lambda(n)n^{-s} = \prod_{p}(1+p^{-s})^{-1} = \zeta(2s)/\zeta(s)$，$s>1$；

(ii) $\sum_{d \mid n} \lambda(d) = \begin{cases} 1, & n \text{ 是平方数}, \\ 0, & \text{其它}; \end{cases}$

(iii) $\sum_{mn=l} \mu^2(m)\lambda(n) = \begin{cases} 1, & l=1, \\ 0, & l>1. \end{cases}$

6．证明：当 $s>1$ 时 $\sum_{n=1}^{\infty} \tau(n)n^{-s} = \zeta^2(s)$。

7．证明：当 $s>2$ 时，$\sum_{n=1}^{\infty} \phi(n)n^{-s} = \zeta(s-1)/\zeta(s)$。由此

给出$\sum_{d \mid n}\phi(d)=n$及$\sum_{d \mid n}\mu(d)/d=\phi(n)/n$的新证明。

8．设$s>1$。证明：(i) $-\zeta'(s)/\zeta(s)=\sum_{n=1}^{\infty}\Lambda(n)n^{-s}$；

(ii) 由(i) 给出$\sum_{d \mid n}\Lambda(n)=\ln n$及$\Lambda(n)=-\sum_{d \mid n}\mu(d)\ln d$的新证明。

第九章 数论函数

在前面八章中，经常出现自变数 n 在某个整数集合中取值，应变数 y 取复数值的函数 $y=f(n)$，这种函数我们称之为数论函数或算术函数，它们在研究许多数论问题中起着十分重要的作用，数论函数是数论的一个重要研究课题，是研究各种数论问题不可缺少的工具。因此，在本书的最后一章对数论函数作一个初步的一般性讨论，介绍有关基础知识，以及几个重要数论函数的性质。

数论函数的定义域可以取各种形式的整数集合。为了简单起见，当我们不说明定义域时，这个数论函数的定义域就是全体正整数集合 $\boldsymbol{N}$，而在其它情形则将明确指出其定义域。

§1 积性函数

定义1 定义在集合 D 上的数论函数 $f(n)$ 称为是**积性函数**，如果满足

$$f(mn)=f(m)f(n),\qquad (m,n)=1,\ m,n\in D; \tag{1}$$

称为是**完全积性函数**，如果满足

$$f(mn)=f(m)f(n),\qquad m,n\in D. \tag{2}$$

这是一类重要的数论函数。例如：$y=n^k$（k 是给定的非负整数），$n\in\boldsymbol{Z}$；$y=n^{-k}$（k 是给定的正整数），$n\in\boldsymbol{Z}$，$n\neq 0$；$y=n^s$（s 给定的实数），$n\in\boldsymbol{N}$ 等都是完全积性函数。第六章§3式(3)给出的 $h(d),d\in\boldsymbol{Z}$，也是完全积性函数，这是因为

$$h(d_1d_2)=h(d_1)h(d_2)=0,\quad 当\ 2\mid d_1d_2;$$

以及当 $2\nmid d_1d_2$ 时，由

$$\frac{d_1d_2-1}{2}\equiv\frac{d_1-1}{2}+\frac{d_2-1}{2}\pmod 2$$

推出

$$h(d_1d_2)=h(d_1)h(d_2),\qquad 当\ 2\nmid d_1d_2.$$

此外，第四章§6的Legendre符号$\left(\frac{n}{p}\right)$，$n\in Z$；第四章§7的Jacobi符号$\left(\frac{n}{P}\right)$，$n\in \boldsymbol{Z}$，也都是完全积性的。下面几个数论函数是积性的，但不是完全积性的①：第一章§6的除数函数$\tau(n)$（见习题六第7题）；第一章§6的除数和函数$\sigma(n)$（见习题六第7题）；第三章§3的Euler函数$\phi(n)$（见式(4)）；以及第八章§1的Möbius函数$\mu(n)$（见式(26)）。请读者自己举例说明它们不是完全积性的。数论函数$e^{2\pi ian/m}$（$a,m\neq 0$是给定整数），$n\in \boldsymbol{Z}$，当$m\nmid a$时不是积性的。$\ln n$，及第八章§2的Mangoldt函数$\Lambda(n)$也都不是积性的（请读者验证）。

我们再来举几个例子。第四章§4定理1中的同余方程的解数$T(m;f)$是m的积性函数（见式(3)），一般说来它不是完全积性的（为什么）。第一章§8中的$\alpha(p;n)$（p是给定的素数）——整除$n!$的p的最高次幂——是一个数论函数，但不是积性的（为什么）。对给定的模m，第五章§1中给出的a对模m的指数$\delta_m(a)$是定义在$a\in \boldsymbol{Z}$，$(a,m)=1$上的数论函数，当$m=1,2$时是完全积性的；当$m>2$时不是积性函数（为什么）。设p为奇素数，k为正整数，g为模p^k的原根。第五章§3中的$\gamma(a)=\gamma_{p^k,g}(a)$（以原根$g$为底的$a$对模$p^k$的指标）是定义在$a\in \boldsymbol{Z}$，$(a,p)=1$上的数论函数，它不是积性函数（为什么），但对任意整数c，

$$\chi(a;p^k)=\begin{cases}\exp(2\pi ic\gamma(a)/\phi(p^k)), & (a,p)=1,\\ 0, & (a,p)>1,\end{cases}\tag{3}$$

① 它们的定义域都是N，所以不写出了。以后均这样。

是定义在 $a\in \mathbf{Z}$ 上的完全积性函数。因为当 $(a_1a_2,p)>1$ 时，显然有

$$\chi(a_1a_2;p^k)=\chi(a_1;p^k)\chi(a_2;p^k)=0;$$

当 $(a_1a_2,p)=1$ 时，由第五章§3性质 2 $(m=p^k)$ 推出

$$\begin{aligned}\chi(a_1a_2;p^k)&=\exp(2\pi i\, c\gamma(a_1a_2)/\phi(p^k))\\&=\exp(2\pi i c(\gamma(a_1)+\gamma(a_2))/\phi(p^k))\\&=\chi(a_1;p^k)\chi(a_2;p^k).\end{aligned}$$

还有两个重要的数论函数是 $\omega(n)$ 和 $\Omega(n)$。设 $n>1$ 的标准素因数分解式是

$$n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}. \tag{4}$$

我们定义

$$\omega(n)=\begin{cases} r, & n>1,\\ 0, & n=1,\end{cases} \tag{5}$$

即 $\omega(n)$ 是 n 的不同的素因数的个数；以及

$$\Omega(n)=\begin{cases} \alpha_1+\cdots+\alpha_r, & n>1,\\ 0, & n=1,\end{cases} \tag{6}$$

即 $\Omega(n)$ 是 n 的全部素因数的个数（即按重数计算）。这两个数论函数都不是积性函数，但容易验证：

$$\omega(mn)=\omega(m)+\omega(n),\qquad (m,n)=1, \tag{7}$$

及对任意的正整数 m,n 有

$$\Omega(mn)=\Omega(m)+\Omega(n). \tag{8}$$

由式(7)和(8)立即推出数论函数

$$\nu(n)=(-1)^{\omega(n)} \tag{9}$$

是积性函数，但不是完全积性的，而数论函数

$$\lambda(n)=(-1)^{\Omega(n)} \tag{10}$$

是完全积性函数。$\lambda(n)$ 通常称为 Liouville 函数。

显见，两个(完全)积性函数之积及商(分母恒不为零)都是(完全)积性函数。积性函数的构造是十分简单的。为了简单起

见，下面仅讨论定义域为N的情形。

定理1 设$f(n)$是不恒为零的数论函数，$n>1$时由式(4)给出。那么，$f(n)$是积性函数的充要条件是$f(1)=1$，及

$$f(n)=f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r});\tag{11}$$

$f(n)$是完全积性的充要条件是$f(1)=1$及

$$f(n)=f^{\alpha_1}(p_1)\cdots f^{\alpha_r}(p_r).\tag{12}$$

证 *必要性* 由条件知必有$f(n_0)\neq 0$。由式(1)得

$$0\neq f(n_0)=f(1\cdot n_0)=f(1)\cdot f(n_0),$$

这就推出$f(1)=1$，式(11)和式(12)分别由式(1)和(2)推出。

充分性 当m,n中有一个等于1时，不妨设$m=1$，由$f(1)=1$推出式(1)和(2)一定成立。当$n>1$，$m>1$时，设m的素因数分解式是$q_1^{\beta_1}\cdots q_s^{\beta_s}$。若式(11)成立，那么当$(m,n)=1$时，$mn$的素因数分解式是$q_1^{\beta_1}\cdots q_s^{\beta_s}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$。由式(11)得

$$\begin{aligned}f(mn)&=f(q_1^{\beta_1}\cdots q_s^{\beta_s}p_1^{\alpha_1}\cdots p_r^{\alpha_r})\\&=f(q_1^{\beta_1})\cdots f(q_s^{\beta_s})f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r})\\&=f(m)f(n),\end{aligned}$$

即式(1)成立，所以$f(n)$是积性函数。若式(12)成立，假定$p_1=q_1,\cdots,p_t=q_t$，以及当$j>t$时总有$p_j\neq q_i$，$1\leqslant i\leqslant s$，和$q_j\neq p_i$，$1\leqslant i\leqslant r$。这样，mn的素因数分解式是

$$p_1^{\alpha_1+\beta_1}\cdots p_t^{\alpha_t+\beta_t}q_{t+1}^{\beta_{t+1}}\cdots q_s^{\beta_s}p_{t+1}^{\alpha_{t+1}}\cdots p_r^{\alpha_r},$$

由式(12)得

$$\begin{aligned}f(mn)&=f^{\alpha_1+\beta_1}(p_1)\cdots f^{\alpha_t+\beta_t}(p_t)f^{\beta_{t+1}}(q_{t+1})\cdots f^{\beta_s}(q_s)\\&\quad\times f^{\alpha_{t+1}}(p_{t+1})\cdots f^{\alpha_r}(p_r)\\&=f^{\beta_1}(q_1)\cdots f^{\beta_s}(q_s)f^{\alpha_1}(p_1)\cdots f^{\alpha_r}(p_r)\\&=f(m)f(n),\end{aligned}$$

这就证明了$f(n)$是完全积性的。证毕。

对于一个数论函数$f(n)$，可以先证明它是积性的，然后利

用式(11)或(12)(如果是完全积性的)，得到它的表达式。例如，对 $\phi(n)$ 就是在第三章§3式(4)证明了它是积性的，及在第三章§2定理8给出了 $\phi(p^a)$ 的公式，而得到它的表达式——第三章§3式(5)——的。反过来，我们也可以证明它有式(11)或(12)成立及 $f(1)=1$，然后推出 $f(n)$ 是积性的或完全积性的。在第八章§1的式(25)及(27)正是证明了对 $\phi(n)$ 有表达式(11)(即第三章§3式(5)成立，由此即可推出它是积性的。这是讨论积性函数的两个途径。对于 $\tau(n)$ 和 $\sigma(n)$，第一章§6的式(7)和式(8)正是证明了对它们式(11)成立，由此从定理1的充分性就推出它们是积性函数。当然也可直接证明 $\tau(n)$ 和 $\sigma(n)$ 是积性的(请读者自证或见下节定理1(ii))。对于同余方程 $s^2\equiv-1(\bmod n)$ 的解数 $R(n)$，由第四章§4定理1知它是积性函数。第六章§3引理6就是通过求出 $R(p^a)$ 及利用式(11)来得到 $R(n)$ 的表达式(见第六章§3式(23)，(24)及(25))。$R(n)$ 不是完全积性的。

定理1表明：一个积性函数完全由它在素数幂 p^a 上的取值所确定；而完全积性函数则完全由它在素数 p 上的取值所确定。由此可以来构造积性函数。例如，对每个素数 p 定义

$$f(p^a)=\begin{cases}1-p, & a=1,\\ 0, & a>1,\end{cases}$$

$f(1)=1$，及 $n>1$ 由式(4)给出时，

$$f(n)=f(p_1^{a_1})\cdots f(p_r^{a_r}).$$

这就构造了一个数论函数 $f(n)$，由定理1充分性知它是积性的。容易证明：$f(n)=\mu(n)\phi(n)$ (留给读者)。

习 题 一

1. 设 $f(n)$ 是积性函数。证明以下的数论函数都是积性的：

(i) $|f(n)|$；　(ii) $f(n^l)$，l 为任给的正整数；

(iii) $f((n,K))$，K 为给定的整数；(iv) 对给定整数 K，定义

$$f_1(n)=\begin{cases}0, & (n,K)>1,\\ f(n), & (n,K)=1;\end{cases}$$

(v) 对给定整数 K，定义 $f_2(n)=f(n^*)$，这里 $n=n^*m$，$(n^*,K)=1$，及 m 满足：若素数 $p|m$ 则必有 $p|K$。

2. 若 $f(n)$ 是积性函数，则

$$f(m)f(n)=f((m,n))f([m,\ n])。$$

3. 若积性函数 $f(n)$ 在 $n=-1$ 有定义，则 $f(-1)=\pm1$。

4. 设 k 是给定的正整数，定义正整数集合上的函数

$$P_k(n)=\begin{cases}1, & n\text{ 是 }k\text{ 次方数},\\ 0, & \text{其它}。\end{cases}$$

证明：$P_k(n)$ 是积性的，且仅当 $k=1$ 时是完全积性的。此外，

$$P_k(n)=[n^{1/k}]-[(n-1)^{1/k}],\quad P_1(n)\equiv1。$$

5. 设 k 是给定的正整数，定义正整数集合上的函数

$$Q_k(n)=\begin{cases}1, & n\text{ 无大于 1 的 }k\text{ 次方因数},\\ 0, & \text{其它}。\end{cases}$$

证明：$Q_k(n)$ 是积性的，且仅当 $k=1$ 时是完全积性的。此外，

$$Q_1(n)=[1/n],\quad Q_2(n)=|\mu(n)|=\mu^2(n)=\mu(n)\nu(n)。$$

6. 设 l 是给定的正整数。以 $\tau_l(n)$ 表示正整数 n 表为 l 个正整数 $d_1,d_2,\cdots,d_l$ 的乘积的不同的表法个数。例如，$\tau_1(n)\equiv1$，$\tau_2(n)=\tau(n)$。证明：$\tau_l(n)$ 是积性函数，且当 $l\geqslant2$ 时不是完全积性的。试求 $\tau_l(n)$ 的表示式。

7. 设 l 是给定的正整数。以 $\tau_l^*(n)$ 表示以下表法的个数：$n=d_1\cdots d_l$，$(d_i,d_j)=1$，$i\neq j$，d_i 为正整数。证明：$\tau_l^*(n)$ 是积性函数，且当 $l\geqslant2$ 时不是完全积性的。试求 $\tau_l^*(n)$ 的表示式。

8. 以 $T(n)$ 表 $x^2+x\equiv0\pmod n$ 的解数。求 $T(n)$ 的表示式。

§2 Möbius变换及其反转公式

对于给定的数论函数 $f(n)$，我们经常要考虑与它相关的一个新的数论函数：

$$F(n)=\sum_{d\mid n}f(d). \qquad (1)$$

例如：取 $f(n)\equiv 1$，则 $F(n)=\tau(n)$；$f(n)=n$，$F(n)=\sigma(n)$；$f(n)=\phi(n)$，$F(n)=n$(第三章§3定理2)；$f(n)=\mu(n)$，$F(n)=[1/n]$(第八章§1引理2)；$f(n)=\Lambda(n)$，$F(n)=\ln n$（第八章§2引理8）；以及取 $f(n)=h(n)$，则$F(n)=N(n)/4$(第六章§3定理1)。通常把数论函数 $F(n)$称为是数论函数 $f(n)$的 Möbius变换，而把 $f(n)$称为是 $F(n)$的 Möbius逆变换。这里的两个基本问题是：(A）给定了 $f(n)$，如何求 $F(n)$的表达式，及 $F(n)$有怎样的性质；(B）反过来，给定了 $F(n)$，能不能找到$f(n)$使式(1）成立，如果存在的话，它是不是唯一的。上面所举的例子实际上已经具体地回答了问题(A)，而对问题(B)只讨论了一个特殊例子 $F(n)=N(n)/4$。我们先来讨论问题(A)。

定理1 设 $f(n)$是给定的数论函数，$F(n)$是它的 Möbius 变换。那么

(i) $F(1)=f(1)$，当 $n>1$ 由§1式(4)给出时，

$$F(n)=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}f(p_1^{e_1}\cdots p_r^{e_r}). \qquad (2)$$

(ii) $f(n)$是积性函数则 $F(n)$也是积性函数，且当 $n>1$由§1式(4)给出时，

$$F(n)=\prod_{j=1}^{r}(1+f(p_j)+\cdots+f(p_j^{\alpha_j}))$$

$$=\prod_{p^{\alpha}\| n}(1+f(p)+\cdots+f(p^{\alpha}))\,; \qquad (3)$$

$f(n)$是完全积性函数时，

$$F(n)=\prod_{j=1}^{r}(1+f(p_j)+\cdots+f^{\alpha_j}(p_j))$$

$$=\prod_{p^\alpha\|n}(1+f(p)+\cdots+f^\alpha(p)).\qquad(4)$$

证 $F(1)=f(1)$是显然的。式(2)就是第一章§6式(21)。这就证明了(i)。当$f(n)$是积性函数时，由式(2)得

$$F(n)=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}\{f(p_1^{e_1})\cdots f(p_r^{e_r})\}$$

$$=\left\{\sum_{e_1=0}^{\alpha_1}f(p_1^{e_1})\right\}\cdots\left\{\sum_{e_r=0}^{\alpha_r}f(p_r^{e_r})\right\},$$

这就证明了式(3)。由式(3)显然可得

$$F(n)=F(p_1^{\alpha_1})\cdots F(p_r^{\alpha_r}).\qquad(5)$$

由此及§1定理1(注意$F(1)=f(1)=1$)就推出$F(n)$是积性函数。当$f(n)$是完全积性函数时，由式(3)推出式(4)。这就证明了(ii)。

由$f(n)$是积性函数推出$F(n)$是积性函数还可用下面的方法直接证明，并由此推出(ii)的其它结论。这依赖于下面的引理。

引理2 设$(m,n)=1$，k是给定的正整数。那么，对每个正整数d有$d^k|mn$成立的充要条件是存在唯一的一对正整数d_1,d_2满足

$$d=d_1d_2,\quad d_1^k|m,\quad d_2^k|n.\qquad(6)$$

证 我们利用第一章§4例6(ii)中的结论(即第一章§6推论5)来证。由$(m,n)=1$知$d^k|mn$的充要条件是

$$d^k=(d^k,mn)=(d^k,m)(d^k,n).\qquad(7)$$

显见，$((d^k,m),(d^k,n))=1$，故由第一章§4例6(ii)知

$$(d^k,m)=((d^k,m),d)^k=(d,m)^k,\qquad(8)$$

$$(d^k,n)=((d^k,n),d)^k=(d,n)^k. \tag{9}$$

取 $d_1=(d,m)$， $d_2=(d,n)$， 由以上三式就推出式(6)成立。 反过来，若有式(6)成立，$d^k|mn$ 是显然的。进而由式(7)，(8)，(9)知，

$$d_1^k d_2^k=(d^k,m)(d^k,n)=(d,m)^k(d,n)^k.$$

由此，注意到 $(m,n)=1$， $(d_1,n)=(d_2,m)=1$ 就推出

$$d_1=(d,m),\quad d_2=(d,n).$$

证毕。

定理1(ii)的另一证明 设 $(m,n)=1$。由引理2（取 $k=1$）及 $f(n)$ 是积性函数得

$$F(mn)=\sum_{d|mn}f(d)=\sum_{d_1|m}\sum_{d_2|n}f(d_1d_2)$$

$$=\sum_{d_1|m}f(d_1)\sum_{d_2|n}f(d_2)=F(m)F(n). \tag{10}$$

这就证明了 $F(n)$ 也是积性的。因此，当 $n>1$ 由§1式(4)给出时就有式(5)成立。由此即推得式(3)和式(4)。

下面来举几个例子。

例 1 求 Liouville 函数 $\lambda(n)$ 的 Möbius 变换。

解

$$\sum_{d|p^\alpha}\lambda(d)=(-1)^0+(-1)^1+\cdots+(-1)^\alpha=\begin{cases}1, & 2|\alpha,\\ 0, & 2\nmid\alpha.\end{cases} \tag{11}$$

由此及 $\lambda(n)$ 是积性函数得

$$\sum_{d|n}\lambda(d)=\begin{cases}1, & n\text{ 是完全平方},\\ 0, & \text{其它}.\end{cases} \tag{12}$$

例 2 求 $\mu^2(n)/\varphi(n)$ 的 Möbius 变换。

解

$$\sum_{d|p^\alpha}\mu^2(d)/\varphi(d)=1+1/(p-1)=(1-1/p)^{-1}.$$

由此及 $\mu^2(n)/\phi(n)$ 是积性函数得

$$\sum_{d\mid n}\mu^2(d)/\phi(d)=\prod_{p\mid n}(1-1/p)^{-1}=n/\phi(n)。\tag{13}$$

例 3 求 $\Omega(n)$ 的 Möbius 变换 $F(n)$。

解 $\Omega(n)$ 不是积性函数。只能利用式(2)计算。$F(1)=0$，$1<n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ 时，

$$\begin{aligned}F(n)&=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}\Omega(p_1^{e_1}\cdots p_r^{e_r})\\&=\sum_{e_1=0}^{\alpha_1}\cdots\sum_{e_r=0}^{\alpha_r}(e_1+\cdots+e_r)\\&=\frac{1}{2}\alpha_1(\alpha_1+1)\cdots(\alpha_r+1)+\cdots+\frac{1}{2}\alpha_r(\alpha_1+1)\cdots(\alpha_r+1)\\&=\frac{1}{2}\Omega(n)\tau(n)。\end{aligned}$$

定理1(ii)的两个有用的特殊情形是：

推论3 设 $f(n)$ 是积性函数。我们有

$$\sum_{d\mid n}\mu(d)f(d)=\prod_{p\mid n}(1-f(p)),\tag{14}$$

及

$$\sum_{d\mid n}\mu^2(d)f(d)=\prod_{p\mid n}(1+f(p))。\tag{15}$$

证明留给读者。例 2 就是式(15)的例子。取 $f(n)=1/n$，由式(14)即得

$$\sum_{d\mid n}\mu(d)/d=\prod_{p\mid n}\left(1-\frac{1}{p}\right),\tag{16}$$

这就是第八章§1式(27)，证明也相同。由此及第三章§3式(5)推出

$$\phi(n)=\sum_{d\mid n}\mu(d)(n/d). \tag{17}$$

这就是第八章§1式(25)。取 $f(n)\equiv 1$，由式(14)得

$$I(n)=\sum_{d\mid n}\mu(d)=\begin{cases}1, & n=1,\\ 0, & n>1.\end{cases} \tag{18}$$

(我们用 $I(n)$ 表示这个数论函数)。这给出了第八章§1式(24)又一证明。

下面来讨论问题(B)。我们要证明

定理4 对每个给定的数论函数 $F(n)$，一定存在唯一的数论函数 $f(n)$，使得式(1)成立，且

$$f(n)=\sum_{d\mid n}\mu(d)F(n/d). \tag{19}$$

即数论函数 $F(n)$ 的 Möbius 逆变换 $f(n)$ 是存在唯一的，且由式(19)给出。

证 先来证唯一性。若有 $f_1(n), f_2(n)$ 均使式(1)成立，设 $f(n)=f_1(n)-f_2(n)$，则有

$$\sum_{d\mid n}f(d)=0.$$

用归纳法来证 $f(n)$ 恒等于零。由上式知 $f(1)=0$，所以结论对 $n=1$ 成立。假设当 $1\leqslant n<k\ (k\geqslant 2)$ 时必有 $f(n)=0$。当 $n=k$ 时，由上式得

$$0=\sum_{\substack{d\mid k\\ d<k}}f(d)+f(k).$$

由此及归纳假设即得 $f(k)=0$。所以 $f(n)$ 恒等于零，即 $f_1(n)=f_2(n)$。这就证明了唯一性。

下面来证存在性，且 $f(n)$ 必由式(19)给出。由于已经证明了唯一性，所以只要直接验证由式(19)定义的 $f(n)$ 满足式(1)。我们有

$$\sum_{d\mid n}f(d)=\sum_{d\mid n}\left\{\sum_{k\mid d}\mu(k)F(d/k)\right\}$$

$$=\sum_{k\mid n}\mu(k)\sum_{k\mid d,d\mid n}F(d/k).$$

令 $d=kl$ 得

$$\sum_{d\mid n}f(d)=\sum_{k\mid n}\mu(k)\sum_{l\mid n/k}F(l)$$

$$=\sum_{l\mid n}F(l)\sum_{k\mid n/l}\mu(k)=F(n),$$

即式(1)成立，最后一步用到了式(18)。证毕。

关于定理4的证明，我们要说明两点。第一，$f(n)$的存在性可以直接用归纳定义的方法来证明，但不能得到表达式(19)。这就是：定义 $f(1)=F(1)$。假设 $f(1),\cdots,f(k-1)\ (k\geqslant 2)$ 都已定义，则定义

$$f(k)=F(k)-\sum_{d\mid k,d<k}f(d).\tag{20}$$

这样，就归纳地确定了一个数论函数 $f(n)$。由 $f(1)=F(1)$及式(20)就推出式(1)成立。第二，定理4的证明没有说明 $f(n)$的表达式是如何来的。下面来解释这一点。Möbius 函数的性质——式(18)在数论函数研究中起着极为重要的作用，在第八章§1中已看到了这一点。这一性质能把"等于1的元素留下"，把"大于1的元素去掉"。利用这一点，我们有

$$f(n)=\sum_{k\mid n}f(n/k)\sum_{d\mid k}\mu(d)$$

$$=\sum_{d\mid n}\mu(d)\sum_{d\mid k,k\mid n}f(n/k).$$

令 $k=dl$ 得

$$f(n)=\sum_{d\mid n}\mu(d)\sum_{l\mid n/d}f((n/d)/l).$$

由此可以看出，为使式(1)成立，就应有式(19)成立。

由于当 d 和 n/d 同时遍历 n 的正除数，所以式(19)也可以写为

$$f(n)=\sum_{d\mid n}\mu(n/d)F(d). \tag{21}$$

这样，由定理 4 及本节开始所说的例子就得到：

$$1=\sum_{d\mid n}\mu(d)\tau(n/d)=\sum_{d\mid n}\mu(n/d)\tau(d), \tag{22}$$

$$n=\sum_{d\mid n}\mu(d)\sigma(n/d)=\sum_{d\mid n}\mu(n/d)\sigma(d), \tag{23}$$

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\ln(n/d)=\sum_{d\mid n}\mu(n/d)\ln d, \tag{24}$$

$$h(n)=\sum_{d\mid n}\mu(d)\left(\frac{N(n/d)}{4}\right)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)\left(\frac{N(d)}{4}\right), \tag{25}$$

以及 $F(n)=n$ 的情形即式(17)。

我们可以这样来看式(19)：给定数论函数 $F(n)$，由式(19)就给出了一个新的数论函数 $f(n)$。那么，立刻会提出同样的问题：对每个数论函数 $f(n)$，是否一定有数论函数$F(n)$使式(19)成立，如果存在的话，是否是唯一的。回答是肯定的。这就是：

定理5 对每个给定的数论函数 $f(n)$，一定存在唯一的数论函数 $F(n)$使式(19)成立，且 $F(n)$由式(1)给出。

证 这结论完全可以按照定理 4 那样直接证明，这样的证法留给读者。现在我们用定理 4 来推出这一结论。对给定的 $f(n)$ 由式(1)就确定了一个数论函数 $F(n)$。对这个 $F(n)$和 $f(n)$有式(1)成立，所以由定理 4 知式(19)成立。这就证明了存在性，且由式(1)给出的 $F(n)$满足式(19)。下面来证唯一性。设有 $F_1(n)$，$F_2(n)$使式(19)成立．即

$$f(n)=\sum_{d\mid n}\mu(d)F_1(n/d)=\sum_{d\mid n}\mu(d)F_2(n/d).$$

由定理 4 知，存在唯一的 $f_1(n)$ 和 $f_2(n)$ 使得

$$F_j(n)=\sum_{d\mid n}f_j(d),\quad j=1,2,$$

且

$$f_j(n)=\sum_{d\mid n}\mu(d)F_j(n/d),\quad j=1,2.$$

由以上三式就推出 $f_1(n)=f_2(n)=f(n)$ 及 $F_1(n)=F_2(n)$。这就证明了唯一性。证毕。

同样的，可以利用定理 5 来推出定理 4（留给读者），这两个定理是等价的。概括起来说，定理 4 和定理 5 是证明了：**式(1)和式(19)是等价的**。所以这是一对反转公式，它是很重要的。应该指出，等价性的最简单的证明是直接验证（例如定理 4 存在性的证明）：若式(1)成立，则式(19)一定成立；若式(19)成立则式(1)一定成立，这是很容易证明的，并由此即可推出定理 4、定理 5 成立（留给读者）。这样的证明从形式上看是简单的，我们为了把结论的含意叙述清楚，并介绍初等数论中的一些重要证明方法，所以采用上述的论证。

定理1(ii)证明了 $f(n)$ 是积性函数时，它的 Möbius变换 $F(n)$ 一定也是积性的。那么，反过来是否也对呢？回答是肯定的。这就是

定理6 设 $f(n)$ 是 $F(n)$ 的 Möbius 逆变换。那么，若$F(n)$是积性函数，则 $f(n)$ 也是积性函数。

我们要给出两个证明。一个直接从式(1)出发，另一个利用 $f(n)$ 的表示式(19)。

第一个证明 设$(m,n)=1$。对 mn 用归纳法。当 $mn=1$时，$m=1,n=1$，由此及 $f(1)=F(1)=1$推出结论成立。假设结论对 $mn<l(l\geqslant 2),(m,n)=1$成立，即

$$f(mn)=f(m)f(n),\quad mn<l,(m,n)=1.$$

那么，当 $mn=l,(m,n)=1$时，由式(1)及引理2$(k=1)$得

$$F(mn)=\sum_{d\mid mn}f(d)=\sum_{d_1\mid m}\sum_{d_2\mid n}f(d_1d_2)$$

$$=\sum_{\substack{d_1\mid m\\ d_1d_2<l}}\sum_{d_2\mid n}f(d_1d_2)+f(mn).$$

利用归纳假设、式(1)及 $F(mn)=F(m)F(n)$，由上式得

$$\sum_{d_1\mid m}f(d_1)\sum_{d_2\mid n}f(d_2)=\sum_{\substack{d_1\mid m\\ d_1d_2<mn}}\sum_{d_2\mid n}f(d_1)f(d_2)+f(m)f(n).$$

注意到 $l=mn$，由以上两式推出 $f(mn)=f(m)f(n)$，即结论当 $mn=l$，$(m,n)=1$时也成立。证毕。

第二个证明 设$(m,n)=1$。由定理4知式(19)成立，由此及引理2($k=1$)得

$$f(mn)=\sum_{d\mid mn}\mu(d)F(mn/d)$$

$$=\sum_{d_1\mid m}\sum_{d_2\mid n}\mu(d_1d_2)F(mn/(d_1d_2)).$$

由此及 $\mu(n)$, $F(n)$是积性函数推出（利用$(m,n)=1$，及式(19)）

$$f(mn)=\sum_{d_1\mid m}\mu(d_1)F(m/d_1)\cdot\sum_{d_2\mid n}\mu(d_2)F(n/d_2)$$

$$=f(m)f(n).$$

证毕。

由于积性函数 $F(n)$的 Möbius 逆变换 $f(n)$也是积性的，所以只要求 $f(p^\alpha)$，而这直接从式(1)就可得到

$$f(p^\alpha)=F(p^\alpha)-F(p^{\alpha-1}).\tag{26}$$

当然这也可从式(19)推出。

下面来举几个例子。

例 4 求 $F(n)=n^t$ 的 Möbius 逆变换 $f(n)$。

解 n^t 是积性的，由式(26)得

$$f(p^a)=p^{at}-p^{(a-1)t}=p^{at}(1-p^{-t}).$$

因此有

$$f(n)=n^t\prod_{p\mid n}(1-p^{-t}).$$

例 5 求 $F(n)=\phi(n)$ 的 Möbius 逆变换。

解 $\phi(n)$ 是积性的，由式(26)得

$$f(p^a)=\phi(p^a)-\phi(p^{a-1})=\begin{cases}p(1-2/p), & a=1,\\ p^a(1-p^{-1})^2, & a\geqslant 2.\end{cases}$$

因此有

$$f(n)=n\prod_{p\mid n}\left(1-\frac{2}{p}\right)\prod_{p^2\mid n}\left(1-\frac{1}{p}\right)^2.$$

例 6 求 $F(n)=\Lambda(n)$ 的 Möbius 逆变换 $f(n)$。

解 $\Lambda(n)$ 不是积性的，所以不能用式(26)。但用式(19)要得到 $f(n)$ 的好的表达式较困难。注意到式(24)，我们有

$$\Lambda(n)=\left(\sum_{d\mid n}\mu(d)\right)\ln n-\sum_{d\mid n}\mu(d)\ln d.$$

利用式(18)得

$$\Lambda(n)=-\sum_{d\mid n}\mu(d)\ln d=\sum_{d\mid n}\mu(d)\ln\frac{1}{d},\qquad(27)$$

这就证明了

$$f(n)=\mu(n)\ln(1/n)=-\mu(n)\ln n.$$

例 7 第六章§3的式(29)（或式(35)的前半等式）实际上是证明了 $N(n)/4$ 是积性的。第六章§3的式(2)就是说 $h(n)$ 是 $N(n)/4$ 的 Möbius 逆变换，在那里 $h(n)$ 是直接给出的，而式(2)是直接验证的。现在，我们来指出，通过求 $F(n)=N(n)/4$ 的 Möbius 逆变换 $h(n)$ 就可推出 $h(n)$ 有第六章§3式(3)给出的表达式。由式(26)知

$$h(p^a)=N(p^a)/4-N(p^{a-1})/4,$$

由此及第六章§3式(31),(32)及(33)分别得到

$$h(2^a)=0,\quad a\geqslant 1,$$

$$h(p^a)=1=\left(\frac{-1}{p^a}\right),\quad a\geqslant 1, p\equiv 1(\bmod 4),$$

及

$$h(p^a)=(-1)^a=\left(\frac{-1}{p^a}\right),\quad a\geqslant 1, p\equiv 3(\bmod 4),$$

这里$\left(\frac{-1}{p^a}\right)$是 Jacobi 符号。由此即可推出 $h(n)$ 是完全积性的，并能表为第六章§3式(3)的形式。详细推导留给读者。

例 8 设$P(x)$是整系数多项式，以$S(n;P(x))$表示满足以下条件的整数 d 的个数：

$$(P(d),n)=1,\quad 1\leqslant d\leqslant n.$$

证明：$S(n)=S(n;P(x))$是 n 的积性函数。

证 利用性质(18)有

$$S(n)=\sum_{\substack{d=1\\(P(d),n)=1}}^{n}1=\sum_{d=1}^{n}\sum_{k\mid(P(d),n)}\mu(k)$$

$$=\sum_{k\mid n}\mu(k)\sum_{\substack{d=1\\k\mid P(d)}}^{n}1.$$

以 $T(k)=T(k;P(x))$表同余方程

$$P(x)\equiv 0(\bmod k)$$

的解数。当$k\mid n$时有

$$\sum_{\substack{d=1\\k\mid P(d)}}^{n}1=\frac{n}{k}T(k).$$

因此

$$S(n)=n\sum_{k|n}\mu(k)T(k)/k.$$

由于$T(k)$是k的积性函数（见第四章§4定理1），所以$\mu(k)T(k)/k$也是积性的，进而由定理1(ii)知$S(n)/n$，即$S(n)$也是积性的。若取$F(x)=x$，$S(n)$就是$\phi(n)$。证毕。

Möbius变换可以看作是由全体数论函数组成的集合上的一种运算。求Möbius逆变换所得到的公式(19)或(21)，实际上是一种更一般的数论函数的运算的特殊情形。设f,g是两个数论函数，我们可以考虑新的数论函数

$$H(n)=\sum_{d|n}f(d)g(n/d).\tag{28}$$

我们把数论函数H称为是数论函数f和g的**Dirichlet卷积**，通常简记作

$$H=f*g.\tag{29}$$

显见，当取

$$g(n)=U(n)=1\tag{30}$$

时，这就是f的Möbius变换；当取$g(n)=\mu(n)$时，这就是f的Möbius逆变换，式(17)表明$\phi(n)$是$\mu(n)$和n的Dirichlet卷积。显见，

$$\begin{aligned}f*g(n)&=\sum_{d|n}f(d)g(n/d)=\sum_{d|n}f(n/d)g(d)\\&=\sum_{n=dl}f(d)g(l),\end{aligned}\tag{31}$$

这是卷积的三种表达形式，最后一个和号是表示对n分解为两个正整数d,l的乘积的所有不同的有序的数对$\{d,l\}$求和（例如$3=1\cdot3$和$3=3\cdot1$就是两种不同的分解）。Dirichlet卷积是数论中一个十分重要的工具，它（包括Möbius变换）有各种形式的推广，我们将在习题中安排这方面的部分内容。

习 题 二

1．证明：(i) $\sum_{d\mid n}\tau^3(d)=\left\{\sum_{d\mid n}\tau(d)\right\}^2$；

(ii) $\tau_l(n)=\sum_{d\mid n}\tau_{l-1}(d), l\geqslant 2$，$\tau_l(n)$由习题一第 6 题给出。

2．设 p 是给定的素数，求$\sum_{d\mid n}\mu(d)\mu((d,p))$的表达式。

3．上题中的素数 p 改为整数K，求$\sum_{d\mid n}\mu(d)\mu((d,K))$的表达式。

4．设m是给定的正整数，求$\sum_{d\mid n}\mu(d)\ln^m d$。并证明：当$n$有多于$m$个不同的素因数时，和式等于零。

5．证明：$f(n)$的 Möbius 变换的 Möbius变换为

$$\sum_{d\mid n}f(d)\tau(n/d).$$

6．设$f(n)$是积性函数，k,l 是给定的正整数．证明：

$F_{k,l}(n)=\sum_{d^k\mid n}f(d^l)$是$n$的积性函数。

7．证明：$Q_k(n)=\sum_{d^k\mid n}\mu(d)$，$Q_k(n)$同习题一第 5 题。

8．求$|\mu(n)|$的 Möbius 变换及 Möbius 逆变换。

9．求$P_k(n)$(见习题一第 4 题) 的 Möbius 变换及Möbius逆变换。证明：$P_2(n)$的 Möbius 逆变换是$\lambda(n)$。

10．求$Q_k(n)$(见习题一第 5 题) 的 Möbius 变换及 Möbius 逆变换。

11．以$f(n)$表示满足：$1\leqslant d\leqslant n$，$(d,n)=(d+1,n)=1$的d的个数。证明：$f(n)$是积性函数，且$f(n)=n\prod_{p\mid n}\left(1-\frac{2}{p}\right)$。

12．设 k 是给定的正整数。以 $\phi_k(n)$ 表满足以下条件的数组 $\{d_1,d_2,\cdots,d_k\}$ 的个数：

$$1\leqslant d_j\leqslant n,1\leqslant j\leqslant k \text{ 及 } (d_1,\cdots,d_k,n)=1$$

（显见，$\phi_1(n)=\phi(n)$）。证明：

（i）$\phi_k(n)$ 的 Möbius 变换是 n^k（用两种不同的证法）；

（ii）$\phi_k(n)=n^k\prod\limits_{p\mid n}\left(1-\frac{1}{p^k}\right)$。

13．设 $S_k(n)=n^{-k}\sum\limits_{j=1}^{n}j^k$，$S_k^*(n)=n^{-k}\sum\limits_{\substack{j=1\\(j,n)=1}}^{n}j^k$。

（i）证明 $S_k^*(n)$ 的 Möbius 变换是 $S_k(n)$（用两种方法证）；

（ii）求 $S_1^*(n)$，$S_2^*(n)$ 的值。

14．以下是各种形式的 Möbius 反转公式，它们可以直接验证，也可以利用 $\sum\limits_{d\mid n}\mu(d)=[1/n]$ 来导出。

（i）设 $x\geqslant1$，K 是给定正整数。再设 $1\leqslant n\leqslant x, n\mid K$。证明：$F(n)=\sum\limits_{\substack{d\mid K\\ n\mid d\leqslant x}}f(d)$ 成立的充要条件是 $f(n)=\sum\limits_{\substack{d\mid K\\ n\mid d\leqslant x}}\mu(d/n)F(d)$。

（ii）设实数 $0<x_0\leqslant x_1$，$\alpha(x)$，$\beta(x)$ 是定义在区间 $[x_0,x_1]$ 上的实变数 x 的函数。证明：$\beta(x)=\sum\limits_{1\leqslant d\leqslant x_1/x}\alpha(dx)$ 成立的充要条件是 $\alpha(x)=\sum\limits_{1\leqslant d\leqslant x_1/x}\mu(d)\beta(dx)$，这里 d 是整变数。

（iii）在（ii）中假定 $x_1=+\infty$。那么，$\beta(x)=\sum\limits_{d=1}^{\infty}\alpha(dx)$ 成立的充要条件是 $\alpha(x)=\sum\limits_{d=1}^{\infty}\mu(d)\beta(dx)$，这里假定对给定的 $x\geqslant x_0$，二重级数 $\sum\limits_{d=1}^{\infty}\sum\limits_{k=1}^{\infty}|\alpha(dkx)|$ 及 $\sum\limits_{d=1}^{\infty}\sum\limits_{k=1}^{\infty}|\beta(dkx)|$ 都收敛。

(iv) 设 $\alpha(x),\beta(x)$是定义在 $x\geqslant 1$ 上的函数。证明：$\beta(x)=\sum_{1\leqslant d\leqslant x}\alpha(x/d)$成立的充要条件是$\alpha(x)=\sum_{1\leqslant d\leqslant x}\mu(d)\beta(x/d)$，这里 d 是整变数。

(v) 设 $\alpha(x),\beta(x)$是定义在 $x>0$上的函数。证明：$\beta(x)=\sum_{d=1}^{\infty}\alpha(x/d)$成立的充要条件是$\alpha(x)=\sum_{d=1}^{\infty}\mu(d)\beta(x/d)$，这里假定对给定的 $x>0$，二重级数 $\sum_{d=1}^{\infty}\sum_{k=1}^{\infty}\left|\alpha\left(\frac{x}{dk}\right)\right|$ 及$\sum_{d=1}^{\infty}\sum_{k=1}^{\infty}\left|\beta\left(\frac{x}{dk}\right)\right|$ 都收敛。

(vi) 设 $\alpha(x,y),\beta(x,y)$是定义在矩形区域：$0<x_0\leqslant x\leqslant x_1$，$0<y_0\leqslant y\leqslant y_1$ 上的实变数 x,y 的二元函数。证明：

$$\beta(x,y)=\sum_{1\leqslant d\leqslant x_1/x}\ \sum_{1\leqslant l\leqslant y_1/y}\alpha(dx,ly)$$

成立的充要条件是

$$\alpha(x,y)=\sum_{1\leqslant d\leqslant x_1/x}\ \sum_{1\leqslant l\leqslant y_1/y}\mu(d)\mu(l)\beta(dx,ly).$$

(vii) 类似于(ii)推广为(iii),(iv),(v)的形式，对 (vi) 作相应的推广。

15. 设 $h(n)$是完全积性函数，$f(n)$及 $F(n)$是两个数论函数。证明：$F(n)=\sum_{d\mid n}f(d)h(n/d)$成立的充要条件是

$$f(n)=\sum_{d\mid n}\mu(d)F(n/d)h(d).$$

16. 类似于 Möbius 变换的反转公式推广为第15题的形式，把第14题中的各个 Möbius 反转公式作类似的推广。

以下第 17—28 题是关于 Dirichlet 卷积的习题，$U,I,\mu,E,\phi,\tau,\sigma$分别表示数论函数 $U(n)\equiv 1,I(n)=[1/n],\mu(n),E(n)=n,\phi(n),\tau(n),\sigma(n)$。

17. 设 $f_1,\cdots,f_r$ 是数论函数。证明：

(i) $f_1*f_2=f_2*f_1$；

(ii) $(f_1*f_2)*f_3=f_1*(f_2*f_3)$；

(iii) $(f_1+f_2)*f_3=(f_1*f_3)+(f_2*f_3)$，这里"+"号表示函数的加法；

(iv) $f_1*I=f_1$。

18. 设 $h=f*g$。证明：(i) 若 f 和 g 都是积性的，则 h 也是积性的；(ii) 若 h,f 是积性的，则 g 也是积性的。

19. 证明：(i) $\mu*U=I$；(ii) $\tau=U*U$；(iii) $\phi=\mu*E$；
(iv) $\sigma=U*E$；(v) $\sigma=\phi*\tau$；(vi) $\sigma*\phi=E*E$；
(vii) $\tau^2*\mu=\tau*\mu^2$。

20. 设 h 是完全积性函数，hf 表示通常函数的乘法。证明：$h(f*g)=(hf)*(h*g)$。此外，对任意的数论函数 J 有

$$J(f*g)=(Jf)*g+f*(Jg).$$

21. 设 f 是数论函数，$f(1)\neq0$。证明：必有唯一的一个数论函数 g 使得 $f*g=I$。我们称 g 是 f 的**Dirichlet**逆，记作f^{-1}。证明：

$$(f^{-1})^{-1}=f;\qquad (f_1*f_2)^{-1}=(f_1^{-1})*(f_2^{-1}).$$

22. 若 f 是积性函数，则 f^{-1} 也是积性函数。

23. 证明：(i) $\mu^{-1}=U$；(ii) $\tau^{-1}=\mu*\mu$；(iii) 求 E^{-1}；
(iv) 求 σ^{-1},ϕ^{-1}；(v) 求 Liouville 函数 λ 的逆。

24. 设 f 是积性函数。证明：(i) 对每个无平方因子数 n 有 $f^{-1}(n)=\mu(n)f(n)$；(ii) 对每个素数 p 有 $f^{-1}(p^2)=f^2(p)-f(p^2)$。

25. 设 f 是积性函数。证明：f 是完全积性的充要条件是对每个素数 p 及所有整数 $l\geqslant2$ 有 $f^{-1}(p^l)=0$。

26. 设 f 是完全积性函数，g 是一个数论函数，$g(1)\neq0$。证明：(i) $(fg)^{-1}=fg^{-1}$；(ii) $f^{-1}=\mu f$。

27. 设 f 是积性函数。证明：f 是完全积性的充要条件是上题中的(ii)成立。

28. 设 $\phi_1=\mu^2*E$。 证明：$\phi_1(n)=\sum\limits_{d^2\mid n}\mu(d)\sigma(n/d^2)$。

§ 3* 数论函数的均值

一些重要的数论函数的取值是十分不规则的，例如，$\tau(n)$，$\sigma(n)$，$\phi(n)$，$N(n)$，$\mu(n)$，$\Lambda(n)$等，但是它们的均值

$$\sum_{n\leqslant x}f(n) \tag{1}$$

却有很好的渐近公式。本节将讨论$\tau(n)$，$N(n)$，$\phi(n)$，$\mu(n)$及$\Lambda(n)$的均值公式。

定理1 设 $x\geqslant 1$，我们有

$$D(x)=\sum_{n\leqslant x}\tau(n)=x\ln x+r_1(x), \tag{2}$$

其中

$$|r_1(x)|\leqslant x。 \tag{3}$$

证 利用 $\tau(n)=\sum\limits_{d\mid n}1$，即 $\tau(n)$是 $f(n)=1$的 Möbius 变换，可得（作整数变换 $n=dl$）

$$D(x)=\sum_{n\leqslant x}\sum_{d\mid n}1=\sum_{d\leqslant x}\sum_{d\mid n\leqslant x}1=\sum_{d\leqslant x}\sum_{l\leqslant x/d}1 \tag{4}$$

$$=\sum_{d\leqslant x}\left[\frac{x}{d}\right]=x\sum_{d\leqslant x}\frac{1}{d}-\sum_{d\leqslant x}\left\{\frac{x}{d}\right\}, \tag{4'}$$

利用

$$\ln\left(1+\frac{1}{d}\right)<\frac{1}{d}<\ln\left(1+\frac{1}{d-1}\right),\quad d\geqslant 2, \tag{5}$$

可得：对整数 $N\geqslant 1$，

$$1+\ln N \geqslant \sum_{d=1}^{N}\frac{1}{d} \geqslant 1-\ln 2+\ln(N+1). \qquad (6)$$

因此，

$$1 \geqslant \sum_{d \leqslant x}\frac{1}{d}-\ln x \geqslant 1-\ln 2, \quad x \geqslant 1. \qquad (7)$$

由此及式(4′)即证明了所要的结果.

定理1证明了一个余项 $r_1(x)$ 估计很差的渐近公式，下面来改进这结果. 定理1是从式(4)出发来计算 $D(x)$的，现在我们把 $D(x)$表为

$$D(x)=\sum_{n \leqslant x}\sum_{d \mid n}1=\sum_{n \leqslant x}\sum_{dl=n}1, \qquad (8)$$

内层求和号的含意和§2式(31)相同. 现在来看式(8)的几何意义. 在直角坐标平面 uOv 上，内层和表示第一象限内的双曲线 $uv=n$ 上的整点（坐标为整数的点）个数. 因此，式(8)中的二重和表示区域：

$$1 \leqslant u, \quad 1 \leqslant v, \quad uv \leqslant x; \qquad (9)$$

上的整点数（见图1）. 这样，计算 $D(x)$就是计算区域(9)上的整点数. 定理1是这样来计算这些整点的（见图1）：按 $d=1,2,\cdots,[x]$，依次计算直线段

$$u=d, \quad 1 \leqslant v \leqslant x/d$$

上的整点数——$[x/d]$，并把它们加起来. 为了得到渐近公式，我们以 x/d 来近似代替$[x/d]$，这就是式(4′). 当 d 相对于 x 很小时，这样的近似是很精确的，但当 d 比较接近于 x 时，这样的近似就不精确了. 这就是定理1所得到的渐近公式不好的原因. 如果能避免计算大的 d，就有可能改进渐近公式.

我们注意到所讨论的区域(9)对直线 $u=v$ 是对称的. 由图2知，这个区域中的整点数等于区域

$$1 \leqslant u \leqslant \sqrt{x}, \quad 1 \leqslant v \leqslant x/u$$

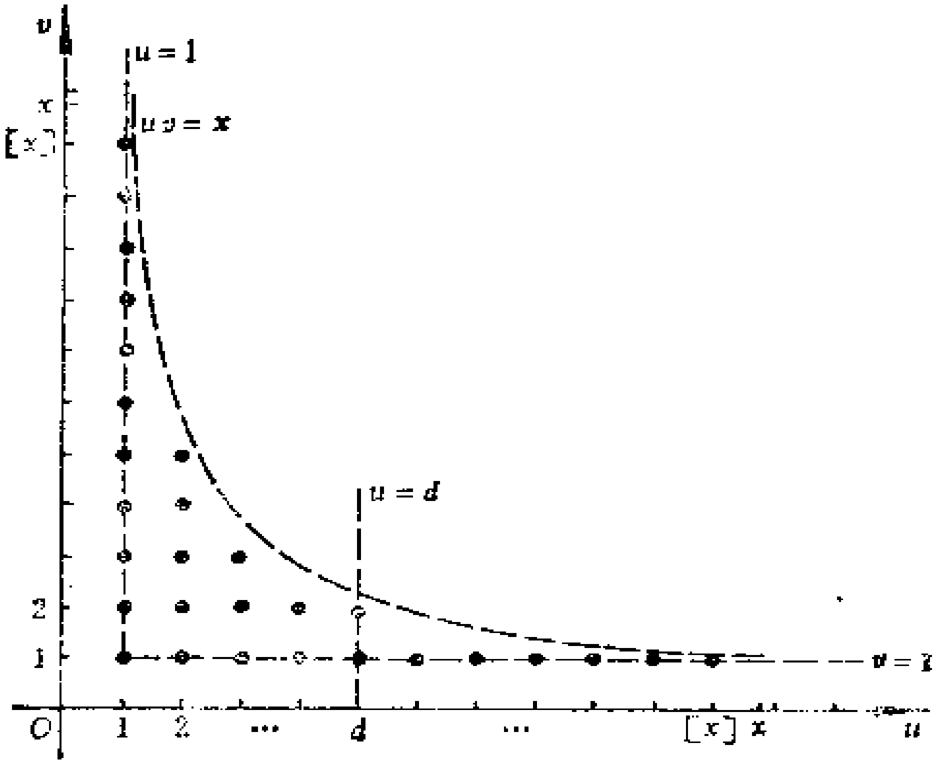


图 1　$x = 11.7$

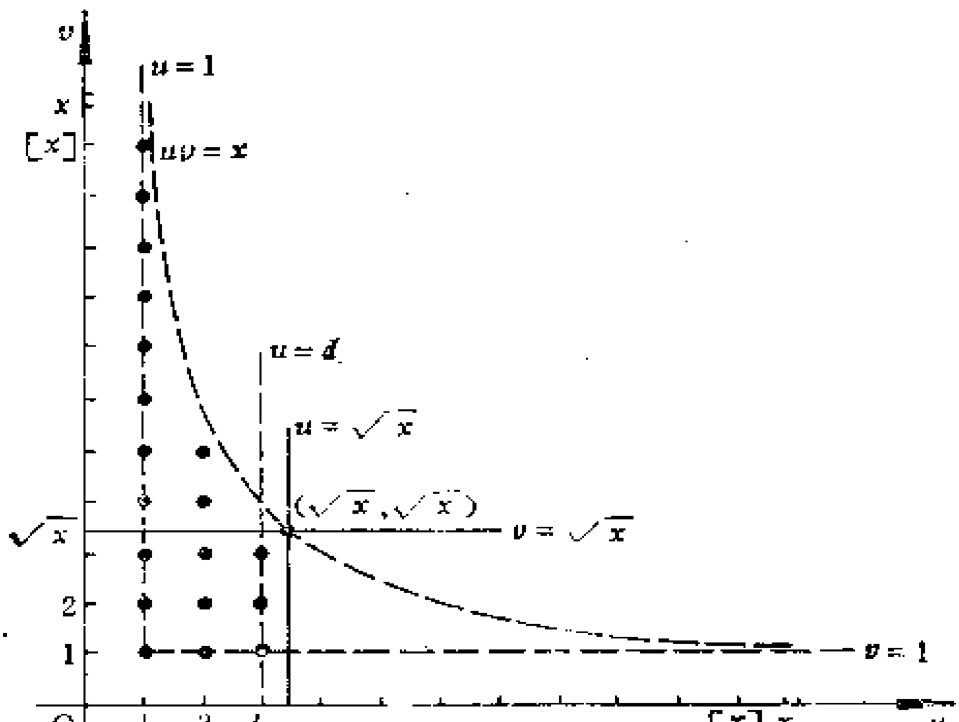


图 2　$x = 11.7$

上的整点数的两倍减去正方形区域

$$1 \leqslant u \leqslant \sqrt{x}, \quad 1 \leqslant v \leqslant \sqrt{x}$$

中的整点数（因为在上面重复计算了一次）。用公式来表示就是：

$$D(x) = \sum_{\substack{dl \leqslant x \\ d \geqslant 1, l \geqslant 1}} 1$$

$$= 2 \sum_{1 \leqslant d \leqslant \sqrt{x}} \sum_{1 \leqslant l \leqslant \frac{x}{d}} 1 - \sum_{1 \leqslant d \leqslant \sqrt{x}} \sum_{1 \leqslant l \leqslant \sqrt{x}} 1$$

$$= 2 \sum_{1 \leqslant d \leqslant \sqrt{x}} \left[\frac{x}{d}\right] - [\sqrt{x}]^2. \tag{10}$$

进而有

$$D(x) = 2x \sum_{1 \leqslant d \leqslant \sqrt{x}} \frac{1}{d} - [\sqrt{x}]^2 - 2 \sum_{1 \leqslant d \leqslant \sqrt{x}} \left\{\frac{x}{d}\right\}$$

$$= 2x \sum_{1 \leqslant d \leqslant \sqrt{x}} \frac{1}{d} - x + 2\sqrt{x}\{x\}$$

$$- \{x\}^2 - 2 \sum_{1 \leqslant d \leqslant \sqrt{x}} \left\{\frac{x}{d}\right\}. \tag{11}$$

这样，为了得到好的渐近公式就归结为要得到式(11)中的调和级数的一个好的渐近公式。为此我们来证明：

引理2 设 $y \geqslant 1$。我们有

$$\sum_{1 \leqslant n \leqslant y} \frac{1}{n} = \ln y + \gamma + \Delta_1(y), \tag{12}$$

这里

$$|\Delta_1(y)| \leqslant 1/y, \tag{13}$$

$$\gamma = \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n} - \frac{1}{t}\right) dt = \int_1^{\infty} \frac{t - [t]}{t[t]} dt$$

$$=0.57721566\cdots, \tag{14}$$

γ 通常称为 Euler 常数。

证 当$y\geqslant 1$时有

$$\sum_{1\leqslant n\leqslant y}\frac{1}{n}-\ln y=\sum_{1\leqslant n\leqslant [y]}\frac{1}{n}-\int_1^y\frac{1}{t}\,dt$$

$$=\sum_{n=1}^{[y]}\int_n^{n+1}\frac{1}{n}\,dt-\int_1^y\frac{1}{t}\,dt$$

$$=\sum_{n=1}^{[y]}\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt+\int_y^{[y]+1}\frac{1}{t}\,dt. \tag{15}$$

由

$$0<\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt<\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{n+1}\right)dt=\frac{1}{n(n+1)} \tag{16}$$

知，级数

$$\sum_{n=1}^{\infty}\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt=\sum_{n=1}^{\infty}\left\{\frac{1}{n}-\ln\left(1+\frac{1}{n}\right)\right\}$$

收敛，设其值为 γ。由式(16)知

$$0<\sum_{n=[y]+1}^{\infty}\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt<\frac{1}{[y]+1}.$$

因而有

$$\Delta_1(y)=\int_y^{[y]+1}\frac{1}{t}dt-\sum_{n=[y]+1}^{\infty}\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt,$$

$$-1/y<-1/([y]+1)<\Delta_1(y)<1/y. \tag{17}$$

这就证明了引理。

由引理 2 及式(11)立即推出

定理3 设$x\geqslant 1$。我们有

$$D(x)=\sum_{n\leqslant x}\tau(n)=x\ln x+(2\gamma-1)x+r_2(x), \tag{13}$$

其中 γ 是由式(14)给出的 Euler 常数，及

$$|r_2(x)|<4\sqrt{x}. \tag{19}$$

证　由式(11)及引理 2 得

$$D(x)=2x(\ln\sqrt{x}+\gamma+\Delta_1(\sqrt{x}))-x$$
$$+2\sqrt{x}\{x\}-\{x\}^2-2\sum_{1\leqslant d\leqslant\sqrt{x}}\left\{\frac{x}{d}\right\}$$
$$=x\ln x+(2\gamma-1)x+r_2(x),$$

其中

$$r_2(x)=2x\Delta_1(\sqrt{x})+2\sqrt{x}\{x\}-\{x\}^2-2\sum_{1\leqslant d\leqslant\sqrt{x}}\left\{\frac{x}{d}\right\}.$$

进而由式(17)推出(利用$0\leqslant\{y\}<1$)

$$-4\sqrt{x}<r_2(x)<4\sqrt{x}.$$

这就证明了所要结论。

如何改进渐近公式(18)中的次要项 $r_2(x)$的估计式(19)，是数论中的一个著名问题，称为Dirichlet 除数问题。

从渐近公式(18)对$\tau(n)$的取值从平均意义上来说能得到什么结果呢？为了看得更清楚，先来证明一个引理。

引理4①　设 $y\geqslant1$。我们有

$$\ln([y]!)=\sum_{1\leqslant n\leqslant y}\ln n=y\ln y-y+\Delta_2(y), \tag{20}$$

其中

$$|\Delta_2(y)|<2+\ln y. \tag{21}$$

证　$1\leqslant y<2$ 时显然成立。可设 $y\geqslant2$。我们有

$$\sum_{1\leqslant n\leqslant y}\ln n=\sum_{2\leqslant n\leqslant[y]}\ln n=\int_1^2\frac{dt}{t}+\int_1^3\frac{dt}{t}+\cdots+\int_1^{[y]}\frac{dt}{t}$$

---

① 这可直接从第八章 § 2式(16)推出。这里给出另一证法。

$$= \int_1^2 \frac{[y]-1}{t}dt + \int_2^3 \frac{[y]-2}{t}dt$$

$$+ \cdots + \int_{[y]-1}^{[y]} \frac{[y]-([y]-1)}{t}dt$$

$$= \int_1^2 \frac{[y]-[t]}{t}dt + \int_2^3 \frac{[y]-[t]}{t}dt$$

$$+ \cdots + \int_{[y]-1}^{[y]} \frac{[y]-[t]}{t}dt$$

$$= [y]\int_1^{[y]} \frac{dt}{t} - \int_1^{[y]} \frac{[t]}{t}dt$$

$$= [y]\ln[y] - ([y]-1) + \int_1^{[y]} \frac{t-[t]}{t}dt.$$

由此及

$$y \ln y \geqslant [y]\ln[y] > (y-1)\ln(y-1)$$

$$= (y-1)\ln y + (y-1)\ln\left(1-\frac{1}{y}\right)$$

$$> y \ln y - \ln y - 1$$

推出

$$2 + \int_1^{[y]} \frac{t-[t]}{t}dt > \Delta_2(y) = [y]\ln[y] - y\ln y + y - [y] + 1$$

$$+ \int_1^{[y]} \frac{t-[t]}{t}dt$$

$$> -\ln y + \int_1^{[y]} \frac{t-[t]}{t}dt,$$

进而得

$$2 + \ln y > \Delta_2(y) > -\ln y.$$

这就证明了所要的结论。

由式(18)和(20)立即推出

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}(\tau(n)-\ln n-2\gamma)=0. \tag{22}$$

这表明：**平均起来说** $\tau(n)$**的值为** $\ln n+2\gamma$，**或者说是** $\ln n$**.**

上面的方法稍作改变就可用来求这样的数论函数 $f(n)$ 的均值：$f(n)$ 是 $g(n)$ 和 $k(n)$ 的 Dirichlet 卷积，即

$$f(n)=\sum_{d\mid n}g(d)k(n/d)=\sum_{dl=n}g(d)k(l),$$

而且 $g(n)$ 和 $k(n)$ 的均值都容易求出。因为，类似于式(8)和(10)可得：

$$\begin{aligned}\sum_{n\leqslant x}f(n)&=\sum_{\substack{dl\leqslant x\\ d\geqslant 1,\ l\geqslant 1}}g(d)k(l)\\&=\sum_{1\leqslant d\leqslant\sqrt{x}}g(d)\sum_{1\leqslant l\leqslant x/d}k(l)\\&\quad+\sum_{1\leqslant l\leqslant\sqrt{x}}k(l)\sum_{1\leqslant d\leqslant x/l}g(d)\\&\quad-\sum_{1\leqslant d\leqslant\sqrt{x}}g(d)\sum_{1\leqslant l\leqslant\sqrt{x}}k(l).\end{aligned} \tag{23}$$

更一般地，若令 $x=st$，$s\geqslant 1$，$t\geqslant 1$，可得

$$\begin{aligned}\sum_{n\leqslant x}f(n)&=\sum_{1\leqslant d\leqslant s}g(d)\sum_{1\leqslant l\leqslant x/d}k(l)\\&\quad+\sum_{1\leqslant l\leqslant t}k(l)\sum_{1\leqslant d\leqslant x/l}g(d)\\&\quad-\sum_{1\leqslant d\leqslant s}g(d)\sum_{1\leqslant l\leqslant t}k(l).\end{aligned} \tag{24}$$

式(4)就是在式(24)中取 $s=x$，$t=1$ 的情形。请读者自己验证式(23)和(24)，并解释它们的几何意义。这样的求和法通常称为

Dirichlet 求和法或双曲型求和法。下面用这方法求$N(n)$和$\phi(n)$的均值。

定理5 设$x\geqslant 1$。我们有

$$C(x)=\sum_{n\leqslant x}N(n)=\pi x+r_3(x), \tag{25}$$

其中

$$-12\sqrt{x}<r_3(x)<12\sqrt{x}. \tag{26}$$

证 由第六章§3定理1及式(23)(取$g(n)=h(n)$, $k(n)\equiv 1$)可得

$$\begin{aligned}\frac{1}{4}C(x)&=\sum_{n\leqslant x}\frac{1}{4}N(n)=\sum_{\substack{dl\leqslant x\\ d\geqslant 1,\ l\geqslant 1}}h(d)\\&=\sum_{1\leqslant d\leqslant\sqrt{x}}h(d)\sum_{1\leqslant l\leqslant x/d}1\\&\quad+\sum_{1\leqslant l\leqslant\sqrt{x}}\sum_{1\leqslant d\leqslant x/l}h(d)\\&\quad-\sum_{1\leqslant d\leqslant\sqrt{x}}h(d)\sum_{1\leqslant l\leqslant\sqrt{x}}1\\&=\Sigma_1+\Sigma_2-\Sigma_3.\end{aligned}$$

下面来计算Σ_1,Σ_2和Σ_3。我们有(利用第六章§3式(3))

$$\begin{aligned}\Sigma_1&=\sum_{1\leqslant d\leqslant\sqrt{x}}h(d)\left[\frac{x}{d}\right]\\&=x\sum_{1\leqslant d\leqslant\sqrt{x}}\frac{h(d)}{d}-\sum_{1\leqslant d\leqslant\sqrt{x}}h(d)\left\{\frac{x}{d}\right\},\end{aligned}$$

$$\sum_{1\leqslant d\leqslant\sqrt{x}}\frac{h(d)}{d}=\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{2j-1}-\sum_{2j-1\geqslant[\sqrt{x}]+1}\frac{(-1)^{j}}{2j-1}.$$

由 arctg y 的幂级数展开式知

$$\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{2j-1}=\frac{\pi}{4}. \tag{27}$$

此外，

$$\frac{-1}{\sqrt{x}}<\frac{-1}{[\sqrt{x}]+1}<\sum_{2j-1\geqslant[x]+1}\frac{(-1)^j}{2j-1}$$

$$<\frac{1}{[\sqrt{x}]+1}<\frac{1}{\sqrt{x}}.$$

由以上各式得

$$\pi x/4-2\sqrt{x}<\Sigma_1<\pi x/4+2\sqrt{x}.$$

由$h(n)$的定义易得，对任意的$y\geqslant 1$，

$$0\leqslant\sum_{1\leqslant d\leqslant y}h(d)\leqslant 1.$$

因此有

$$0\leqslant\Sigma_2\leqslant\sqrt{x},\quad 0\leqslant\Sigma_3\leqslant\sqrt{x}.$$

综合以上各式即得

$$\pi x/4-3\sqrt{x}<C(x)/4<\pi x/4+3\sqrt{x}.$$

这就证明了所要的结论。

由定理 5 立即推出

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\{N(n)-\pi\}=0.$$

这表明平均起来说 $N(n)$的值为π。

由于$N(n)$是不定方程$u^2+v^2=n$的解数，所以均值$C(x)$就是满足$u^2+v^2\leqslant x$的所有整数对$\{u,v\}$个数，因而就是以原点为心、$\sqrt{x}$为半径的圆$R(\sqrt{x})$上的整点数。因此，改进次要项$r_3(x)$的估计通常称为圆内整点问题或Gauss圆问题。这也是数论中的一个著名问题。由此观点可给出定理 5 的一个十分简洁的几何证

明：由于任意一点$\{u,v\}$(不一定是整点)必在整点$\{[u],[v]\}$的右上方的单位正方形上，即以$\{[u],[v]\}$，$\{[u]+1,[v]\}$,$\{[u],[v]+1\}$，$\{[u]+1,[v]+1\}$这四个整点为顶点的正方形上，而点$\{u,v\}$与整点$\{[u],[v]\}$的距离不超过$\sqrt{2}$。因此，对圆 $R(\sqrt{x})$上的每个整点作一个这样的小正方形，那么，这些小正方形两两不重叠(不计边界)，一方面这些小正方形全部覆盖了圆 $R(\sqrt{x}-\sqrt{2})$，另一方面显然这些小正方形全部在圆 $R(\sqrt{x}+\sqrt{2})$中。因此，比较面积(注意小正方形面积为1，所以它们的面积和即为整点数$C(x)$)即得

$$\pi(\sqrt{x}-\sqrt{2})^2 < C(x) < \pi(\sqrt{x}+\sqrt{2})^2. \qquad (28)$$

由此即推出定理 5。应该指出，由式(28)及定理 5 的证明可推出式(27)。请读者自己说明这一点。

下面再来求 $\phi(n)$的均值。如果用§2例5得到的 $\phi(n)$的 Möbius 逆变换，按前面两个例子方法来算，将出现困难。我们要利用$\phi(n)$是$\mu(n)$和 n 的 Dirichlet 卷积，按公式(24)($s=x, t=1$)来做。

定理6 设 $x\geqslant 1$。我们有

$$\Phi(x)=\sum_{n\leqslant x}\phi(n)=\frac{1}{2}\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\right)x^2+r_4(x), \qquad (29)$$

其中

$$|r_4(x)|<3x\ln x+4x. \qquad (30)$$

证 利用§2式(17)，及式(24)(取$s=x, t=1$)可得

$$\Phi(x)=\sum_{n\leqslant x}\sum_{d\mid n}\mu(d)\frac{n}{d}=\sum_{\substack{dl\leqslant x\\ 1\leqslant d,\, l\geqslant 1}}\mu(d)l$$

$$=\sum_{1\leqslant d\leqslant x}\mu(d)\sum_{1\leqslant l\leqslant x/d}l$$

$$=\sum_{1\leqslant d\leqslant x}\mu(d)\cdot\frac{1}{2}\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right).$$

注意到

$$\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right)=\left(\frac{x}{d}-\left\{\frac{x}{d}\right\}\right)\left(\frac{x}{d}-\left\{\frac{x}{d}\right\}+1\right)$$

$$=\frac{x^2}{d^2}+\frac{x}{d}-2\left\{\frac{x}{d}\right\}\frac{x}{d}-\left\{\frac{x}{d}\right\}^2+\left\{\frac{x}{d}\right\}$$

$$=\frac{x^2}{d^2}+\Delta(d,x),$$

及由$0\leqslant\{x/d\}<1$ 和$\{x/d\}\leqslant x/d$ 可得

$$|\Delta(d,x)|\leqslant 3x/d.$$

我们有

$$\Phi(x)=\frac{x^2}{2}\sum_{d\leqslant x}\frac{\mu(d)}{d^2}+\sum_{d\leqslant x}\mu(d)\Delta(d,x),$$

$$\left|\sum_{d\leqslant x}\mu(d)\Delta(d,x)\right|\leqslant 3x\sum_{d\leqslant x}\frac{1}{d}<3x\left(1+\sum_{2\leqslant d\leqslant x}\ln\left(1+\frac{1}{d-1}\right)\right)$$

$$\leqslant 3x(1+\ln[x]),$$

$$\left|\sum_{d>x}\frac{\mu(d)}{d^2}\right|<\sum_{d>x}\frac{1}{d^2}<\sum_{d>x}\left(\frac{1}{d-1}-\frac{1}{d}\right)$$

$$<\frac{1}{[x]}<\frac{2}{x}.$$

由以上三式即得所要结论．证毕．

在式(29)中出现了一个绝对收敛的无穷级数．利用第八章§3式(10)定义的 Riemann ζ 函数、绝对收敛级数的乘法、及第八章§1式(24)可得

$$\zeta(2)\cdot\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\sum_{l=1}^{\infty}\frac{1}{l^2}\cdot\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^2}\sum_{dl=n}\mu(d)=1.$$

由此及第八章 § 2式(9)推出

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=1/\zeta(2)=\prod_p\left(1-\frac{1}{p^2}\right). \tag{31}$$

可以证明：

$$\zeta(2)=\pi^2/6. \tag{32}$$

因而有

$$\Phi(x)=\sum_{n\leqslant x}\phi(n)=\frac{3}{\pi^2}x^2+r_4(x). \tag{33}$$

由此及式(30)推出

$$\left|\frac{1}{x}\sum_{n\leqslant x}\left\{\phi(n)-\frac{6}{\pi^2}n\right\}\right|<3\ln x+5. \tag{34}$$

所以，**平均起来说** $\phi(n)$的值为$6n/\pi^2$。

现在，我们来讨论$\mu(n)$和$\Lambda(n)$的均值。由第八章 § 2定理 7 (ii)知，证明均值 $\psi(x)=\sum\limits_{n\leqslant x}\Lambda(n)$的渐近公式，就等于证明了素数定理。这是很困难的，不能用上面的方法来得到，超出了本书的范围。对$\mu(n)$的均值也是一样。关于这一点只要对它们的Möbius逆变换用Dirichlet求和法作一分析讨论就可看出(留给读者)。但是，在另一方面，它们的Möbius变换都很简单，从它们的Möbius 变换的均值的渐近公式可推出它们本身的某种较弱的加权的均值公式(见式(35)和(37))。

定理7 设 $x\geqslant1$。我们有

$$\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right|\leqslant1. \tag{35}$$

证 由 § 2式(18)得

$$1=\sum_{n\leqslant x}\left[\frac{1}{n}\right]=\sum_{n\leqslant x}\sum_{d\mid n}\mu(d)=\sum_{\substack{d\,l\leqslant x\\ d\geqslant1,\ l\geqslant1}}\mu(d)$$

$$=\sum_{d\leqslant x}\mu(d)\sum_{1\leqslant l\leqslant x/d}1$$

$$=\sum_{d\leqslant x}\mu(d)\left[\frac{x}{d}\right],\tag{36}$$

进而有

$$x\sum_{d\leqslant x}\frac{\mu(d)}{d}=1-\sum_{d\leqslant x}\mu(d)\left\{\frac{x}{d}\right\}.$$

由此及

$$\left|1-\sum_{d\leqslant x}\mu(d)\left\{\frac{x}{d}\right\}\right|=\left|1-\{x\}-\sum_{2\leqslant d\leqslant x}\mu(d)\left\{\frac{x}{d}\right\}\right|\leqslant x$$

就推出式(35)。证毕。

定理8 设 $x\geqslant 1$。我们有

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\ln x+r_5(x),\tag{37}$$

其中

$$|r_5(x)|<4\ln 2+2.$$

证 由第八章§2引理8得

$$\ln([x]!)=\sum_{n\leqslant x}\ln n=\sum_{n\leqslant x}\sum_{d\mid n}\Lambda(d)=\sum_{\substack{dl\leqslant x\\ d\geqslant 1,\ l\geqslant 1}}\Lambda(d)$$

$$=\sum_{d\leqslant x}\Lambda(d)\sum_{1\leqslant l\leqslant x/d}1=\sum_{d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right].$$

(这实际上就是第八章§2的式(39)和(41))。由此及引理4得

$$x\sum_{d\leqslant x}\frac{\Lambda(d)}{d}=x\ln x-x+\Delta_2(x)+\sum_{d\leqslant x}\Lambda(d)\left\{\frac{x}{d}\right\}.$$

由式(21)及第八章§2式(44)推出

$$\left|-x+\Delta_2(x)+\sum_{d\leqslant x}\Lambda(d)\left\{\frac{x}{d}\right\}\right|<(4\ln 2-1)x+\ln x+2,$$

由以上两式就证明了定理。

把式(12)和式(35)相比较，可得出这样的结论：平均起来说 $\mu(n)$ 的取值为零。但由此不能推出

$$\frac{1}{x}\sum_{n\leqslant x}\mu(n)\to 0,\quad x\to+\infty. \tag{38}$$

把式(12)和式(37)相比较，可得出这样的结论：平均起来说 $\Lambda(n)$ 的取值为 1 。但由此不能推出

$$\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\to 1,\quad x\to+\infty. \tag{39}$$

和式(39)一样，式(38)也和素数定理等价。这些超出本书范围我们都不讨论了。从定理 8 可推出一个有用的结论。

定理9 设 $x\geqslant 1$。我们有

$$\sum_{p\leqslant x}\frac{\ln p}{p}=\ln x+r_6(x), \tag{40}$$

其中

$$|r_6(x)|<5\ln 2+3. \tag{41}$$

证 由 $\Lambda(n)$ 的定义知(令 $n=p^m$)

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{p\leqslant x}\frac{\ln p}{p}=\sum_{p^m\leqslant x,\ m\geqslant 2}\frac{\ln p}{p^m}$$

$$<\sum_{p}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\ln p$$

$$=\sum_{p}\frac{\ln p}{p(p-1)}<\sum_{n=2}^{\infty}\frac{\ln n}{n(n-1)}.$$

我们来估计最后的级数：

$$\sum_{n=2}^{\infty}\frac{\ln n}{n(n-1)}=\sum_{n=2}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)\ln n$$

$$=\ln 2+\sum_{n=2}^{\infty}\frac{1}{n}(\ln(n+1)-\ln n)$$

$$= \ln 2 + \sum_{n=2}^{\infty} \frac{1}{n} \ln\left(1 + \frac{1}{n}\right)$$

$$< \ln 2 + \sum_{n=2}^{\infty} \frac{1}{n^2}$$

$$< \ln 2 + \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1 + \ln 2.$$

由以上两式及定理 8 就推出所要的结论。

在第八章§2式(19)我们仅得到了 $\sum_{p \leqslant x} (\ln p)/p$ 的上、下界估计，而式(40)得到了它的渐近公式。由此可以得到 $\sum_{p \leqslant x} 1/p$ 的渐近公式，而在第八章§2式(17)也仅得到了它的上、下界估计。为此需要下面的**Abel求和公式**。

引理10　设 $x \geqslant 1$，$b(n)$ 是一个数论函数，

$$B(x) = \sum_{n \leqslant x} b(n).$$

再设 $a(x)$ 是区间 $[x_1, x_2]$ 上的连续可微函数，$x_2 > x_1 \geqslant 0$。那么有

$$\sum_{x_1 < n \leqslant x_2} b(n) a(n) = B(x_2) a(x_2) - B(x_1) a(x_1) - \int_{x_1}^{x_2} B(x) a'(x) \mathrm{d}x. \tag{42}$$

证　设 $n_1 = [x_1]$，$n_2 = [x_2]$。我们有(约定 $B(0) = 0$)

$$\sum_{x_1 < n \leqslant x_2} b(n) a(n) = \sum_{n_1 < n \leqslant n_2} b(n) a(n)$$

$$= \sum_{n=n_1+1}^{n_2} \{B(n) - B(n-1)\} a(n)$$

$$= -B(n_1) a(n_1 + 1)$$

$$
\begin{aligned}
&-\sum_{n=n_1+1}^{n_2-1} B(n)\ \{a(n+1)-a(n)\}+B(n_2)a(n_2)\\
=&-B(n_1)a(n_1+1)\\
&-\sum_{n=n_1+1}^{n_2-1} B(n)\int_n^{n+1} a'(x)\,\mathrm{d}x+B(n_2)a(n_2)\\
=&-B(n_1)a(n_1+1)\\
&-\int_{n_1+1}^{n_2} B(x)a'(x)\,\mathrm{d}x+B(n_2)a(n_2).
\end{aligned}
$$

此外还有

$$\int_{x_1}^{n_1+1} B(x)a'(x)\,\mathrm{d}x=B(n_1)\{a(n_1+1)-a(x_1)\}.$$

$$\int_{n_2}^{x_2} B(x)a'(x)\,\mathrm{d}x=B(n_2)\{a(x_2)-a(n_2)\}.$$

注意到$B(x_1)=B(n_1)$，$B(x_2)=B(n_2)$，由以上三式即得式(42)。

Abel求和公式(42)表明：如果我们知道了数论函数$b(n)$的均值$B(x)$的渐近公式，那么，对于满足适当条件的函数$a(x)$，数论函数$b(n)a(n)$的均值的渐近公式有可能通过式(42)来得到。例如，取

$$b(n)=\begin{cases}(\ln p)/p, & n=\text{素数 } p,\\ 0, & \text{其它},\end{cases} \tag{43}$$

及$a(x)=(\ln x)^{-1}$，就导致讨论均值$\sum\limits_{p<x}1/p$；若取$a(x)=x$，$b(n)$同上，就导致讨论均值$\sum\limits_{p<x}\ln p$。前者可以得到渐近公式，而后者则不能(后一点请读者自己讨论)。下面来证明：

定理11 设$x\geqslant 2$。我们有

$$\sum_{p<x}\frac{1}{p}=\ln\ln x+A+r_7(x), \tag{44}$$

其中常数

$$A=1-\ln\ln 2+\int_2^{\infty} r_6(t)(t\ \ln^2 t)^{-1}\mathrm{d}t, \tag{45}$$

及

$$|r_7(x)|<2(5\ln 2+3)(\ln x)^{-1}. \tag{46}$$

证　取$x_1=2$，$x_2=x$，$b(n)$由式(43)给出，$a(x)=(\ln x)^{-1}$。由式(42)得

$$\begin{aligned}\sum_{p\leqslant x}\frac{1}{p}&=\frac{1}{2}+\sum_{2<n\leqslant x} b(n)a(n)\\&=\frac{1}{2}+\frac{1}{\ln x}\left\{\sum_{p\leqslant x}\frac{\ln p}{p}\right\}-\frac{1}{2}\\&\quad+\int_2^x\left\{\sum_{p\leqslant t}\frac{\ln p}{p}\right\}\frac{1}{t\ln^2 t}\mathrm{d}t.\end{aligned}$$

由此及式(40)得

$$\begin{aligned}\sum_{p\leqslant x}\frac{1}{p}&=\frac{1}{2}+\frac{1}{\ln x}\{\ln x+r_6(x)\}-\frac{1}{2}\\&\quad+\int_2^x\frac{\mathrm{d}t}{t\ln t}+\int_2^x\frac{r_6(t)}{t\ln^2 t}\mathrm{d}t\\&=\ln\ln x+\left\{1-\ln\ln 2+\int_2^{\infty}\frac{r_6(t)}{t\ln^2 t}\mathrm{d}t\right\}\\&\quad+\frac{r_6(x)}{\ln x}-\int_x^{\infty}\frac{r_6(t)}{t\ln^2 t}\mathrm{d}t.\end{aligned}$$

由式(41)知积分$\int_2^{\infty} r_6(t)(t\ln^2 t)^{-1}\mathrm{d}t$ 收敛，及

$$\left|\frac{r_6(x)}{\ln x}-\int_x^{\infty}\frac{r_6(t)}{t\ln^2 t}\mathrm{d}t\right|<2(5\ln 2+3)\ln^{-1}x.$$

由此及上式就证明了所要结论。

可以证明定理11中的常数

$$A=\gamma+\sum_{p}\{\ln(1-1/p)+1/p\}$$
$$=0.26149721\cdots,\tag{47}$$

其中γ是由式(14)给出的Euler 常数，但已超出本书范围。

Abel求和公式是一个重要的工具，可以用它求许多有用的和式的渐近公式。这些将安排在习题中。

数论函数本身取值不规则的问题，也是一个重要研究课题，这里就不讨论了。有兴趣的读者可见参考书目[2],[3]。

习　题　三

1．证明：$\gamma=1-\int_{1}^{\infty}(t-[t])t^{-2}\mathrm{d}t$，$\gamma$是 Euler 常数。

2．设$x\geqslant 1$。证明：$\sum\limits_{n\leqslant x}\frac{\ln n}{n}=\frac{1}{2}\ln^2 x+c+r(x)$，这里$c$为一常数，$|r(x)|\leqslant A\ln x/x$，$A$为一正常数。

3．设$x\geqslant 2$。证明：$\sum\limits_{n\leqslant x}\sigma(n)=cx^2+r(x)$，$c$为一常数，$|r(x)|\leqslant Ax\ln x$，$A$为一正常数。

4．设$x\geqslant 1$。证明：$\sum\limits_{n\leqslant x}\mu^2(n)=\frac{6}{\pi^2}x+r(x)$，这里$|r(x)|<Ax^{1/2}$，$A$为一正常数。

5．设$D(x)$由§3定理 1 给出。证明：

$$\sum_{n\leqslant x}2^{\omega(n)}=\sum_{n\leqslant\sqrt{x}}\mu(n)D\left(\frac{x}{n^2}\right).$$

6．设$x\geqslant 2$。证明：$\sum\limits_{n\leqslant x}2^{\omega(n)}=\frac{6}{\pi^2}x\ln x+cx+r(x)$，这里$c$为一常数，$|r(x)|\leqslant A\sqrt{x}\ln x$，$A$为一正常数。

7. 求以下均值的渐近公式：

(i) $\sum_{n\leqslant x}\frac{\tau(n)}{n}$； (ii) $\sum_{n\leqslant x}\frac{\sigma(n)}{n}$； (iii) $\sum_{n\leqslant x}\frac{\phi(n)}{n}$；

(iv) $\sum_{n\leqslant x}\frac{2^{\omega(n)}}{n}$； (v) $\sum_{n\leqslant x}\frac{\phi(n)}{n^2}$。

8. 设$x\geqslant 1$。证明：

(i) $\sum_{n\leqslant x}\phi(n)=\frac{1}{2}\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]^2+\frac{1}{2}$；

(ii) $\sum_{n\leqslant x}\frac{\phi(n)}{n}=\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right]$。

9. (i) 证明：当$n\geqslant 2$时，

$$\sigma(n)/n<n/\phi(n)<(\pi^2/6)\sigma(n)/n；$$

(ii) 存在正常数A，使得 $\sum_{n\leqslant x}\frac{n}{\phi(n)}\leqslant Ax$，$x\geqslant 1$；

(iii) 存在正常数B，使得$\sum_{n\leqslant x}\frac{1}{\phi(n)}\leqslant B\ln x$，$x\geqslant 2$。

10. 求均值$\sum_{n\leqslant x}\phi_1(n)$的渐近公式，$\phi_1(n)$由 习题二第28题给出。

11. 在§3引理10的符号和条件下，证明：当取$b(n)\equiv 1$时有

$$\begin{aligned}\sum_{x_1<n\leqslant x_2}a(n)&=\int_{x_1}^{x_2}a(x)\mathrm{d}x+\int_{x_1}^{x_2}(x-[x])a'(x)\mathrm{d}x\\&\quad-(x_2-[x_2])a(x_2)+(x_1-[x_1])a(x_1)\\&=\int_{x_1}^{x_2}a(x)\mathrm{d}x+\int_{x_1}^{x_2}(x-[x]-1/2)a''(x)\mathrm{d}x\\&\quad-(x_2-[x_2]-1/2)a(x_2)\\&\quad+(x_1-[x_1]-1/2)a(x_1).\end{aligned}$$

这一公式通常称为Euler求和公式。利用它来证明§3引理 2 及引理 4 。

12．设实数$s\geqslant 0$，$x\geqslant 1$．证明：$\sum\limits_{n\leqslant x} n^s=\frac{x^{s+1}}{s+1}+r(x)$，$|r(x)|\leqslant x^s$．

13．设实数$s>0$，$s\neq 1$，及$x\geqslant 1$．证明：

$$\sum_{n\leqslant x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+F(s)+r(x),$$

其中$F(s)=\zeta(s)=1-(1-s)^{-1}-s\int_1^{\infty}(t-[t])t^{-s-1}\mathrm{d}t$，及$|r(x)|<x^{-s}$．

14．设实数$s>1$，$x\geqslant 1$．证明：$\sum\limits_{n>x} n^{-s}=\frac{x^{1-s}}{s-1}-r(x)$，$r(x)$同上题．

15．设t为实数，$\sigma_t(n)=\sum\limits_{d\mid n} d^t$．再设$x\geqslant 1$．证明：当$t>0$，$t\neq 1$时，$\sum\limits_{n\leqslant x}\sigma_t(n)=\frac{\zeta(t+1)}{t+1}x^{t+1}+r(x)$，这里$|r(x)|\leqslant A(t)x^{t_1}$，$t_1=\max(1,t)$，$A(t)$是仅和$t$有关的正常数．

16．设$x\geqslant 2$．$\sigma_t(n)$同上题．证明：

(i) $\sum\limits_{n\leqslant x}\sigma_{-1}(n)=\zeta(2)x+r(x)$，$|r_1(x)|\leqslant A_1\ln x$，$A_1$为一正常数；

(ii) 当$t>0$，$t\neq 1$时，$\sum\limits_{n\leqslant x}\sigma_{-t}(n)=\zeta(t+1)x+r_2(x)$，$|r_2(x)|\leqslant A_2(t)x^{t_2}$，这里$A_2(t)$是仅和$t$有关的正常数，$t_2=\max(0,1-t)$．

17．设$x\geqslant 2$．证明：存在正常数A_1使得

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{A_1}{\ln x}+r(x),$$

这里$|r(x)|\leqslant B\ln^{-2}x$，$B$是一正常数．

18. 设$x\geqslant 2$.证明：$\sum\limits_{p\leqslant x}\frac{\ln^2 p}{p}=\frac{1}{2}\ln^2 x+r(x)$，$|r(x)|\leqslant B\ln x$，其中$B$为一正常数。

19. 设$x\geqslant 2$，整数$k\geqslant 2$。求$\sum\limits_{p\leqslant x}\frac{\ln^k p}{p}$的渐近公式。

20. 设$x\geqslant 4$。证明：

$$\sum_{pq\leqslant x}\frac{1}{pq}=(\ln\ln x)^2+A\ln\ln x+r(x),$$

这里求和号表示对两个素变数p,q求和，A是一正常数，$|r(x)|\leqslant B$，B是一正常数。

21. 设$x\geqslant 4$。证明：

(i) $\sum\limits_{n\leqslant x}\omega(n)=x\ln\ln x+A_1x+r_1(x)$；

(ii) $\sum\limits_{n\leqslant x}\Omega(n)=x\ln\ln x+A_2x+r_2(x)$，其中$A_1,A_2$是两个正常数，$|r_j(x)|\leqslant B\pi(x)$，$B$为一正常数。

22. 设$x\geqslant 4$。证明：

$$\sum_{n\leqslant x}\omega^2(n)=x(\ln\ln x)^2+A_3\ln\ln x+r_3(x),$$

其中A_3是一正常数，$|r_3(x)|\leqslant B_1x$，B_1为一正常数。

§4* Dirichlet 特征

我们已经证明过在一些特殊的算术数列中有无穷多个素数，例如，在算术数列$n\equiv 3(\bmod 4)$、$n\equiv -1(\bmod 6)$、$n\equiv 1(\bmod 4)$及$n\equiv 1(\bmod 8)$中都有无穷多个素数，前两个证明很容易，但后两个就不那么简单(见第三章§4习题四第6题，及第四章§6例7)。数论中一个十分著名的问题是要证明：对任意给定的$k>2$及$(a,k)=1$，在算术数列$n\equiv a(\bmod k)$中一定有无穷多个素数。

这一问题已在1837年被 D.G.L.Dirichlet 所解决， 它的证明已超出本书的范围，不能在此讨论。 但是， 为了解决这一问题 Dirichlet 引进了一类十分重要的数论函数，利用它能够从给定的整数序列(例如素数序列)中把属于算术数列 $n\equiv a(\bmod k)$ 的子序列挑选出来。这一节就是要介绍这类数论函数并讨论它的最基本的性质。

定义 1 设 $k\geqslant 1$。$\chi(n)$是定义在全体整数集合上不恒为零的数论函数。如果满足条件：

(i) $\chi(n)=0$, 当$(n,k)>1$;

(ii) 是周期为 k 的周期函数：$\chi(n+k)=\chi(n)$;

(iii) 是完全积性函数：对任意整数m,n有$\chi(mn)=\chi(m)\chi(n)$,

那么，$\chi(n)$就称为是模 k 的 **Dirichlet 特征或模 k 的剩余特征**，简称为**模 k 的特征**。为明确起见，以 $\chi(n;k)$或$\chi \bmod k$ 表模 k 的特征。

例如，Legendre 符号$\left(\frac{n}{p}\right)$就是模 p 的特征，Jacobi 符号$\left(\frac{n}{P}\right)$是模 P 的特征，§1式(3)给出的 $\chi(a;p^k)$是模 p^k 的特征(为什么)，以及第六章§3式(3)定义的 $h(n)$是模 4 的特征。

由 $\chi(n)$是积性的且不恒为零知(§1定理1)

$$\chi(1)=1, \tag{1}$$

以及由 $\chi(-1)\cdot\chi(-1)=\chi(1)$推出

$$\chi(-1)=\pm 1. \tag{2}$$

由Euler定理$n^{\phi(k)}\equiv 1(\bmod k)$、周期性及完全积性推出：当$(n,k)=1$时，

$$1=\chi(1)=\chi(n^{\phi(k)})=(\chi(n))^{\phi(k)}. \tag{3}$$

由定义立即推出：模 1 的特征只有一个，即

$$\chi(n;1)=1,\quad n\in \boldsymbol{Z}. \tag{4}$$

由 $\chi(2m+1;2)=\chi(1;2)=1$ 知，模 2 的特征也只有一个，即

$$\chi(n,2)=\begin{cases}1, & 2\nmid n,\\ 0, & 2\mid n.\end{cases} \tag{5}$$

显见，要确定一个特征就只要确定它在模 k 的既约剩余系上的取值，且这样的取值满足完全积性条件。下面来举几个例子。模 3 的特征可能的取值是：

$$\chi(1;3)=1,$$

及由完全积性条件知 $\chi^2(2;3)=\chi(4;3)=\chi(1;3)=1$，所以

$$\chi(2;3)=\pm 1.$$

所以模 3 特征有两个：

$$\chi(n;3,0)=\begin{cases}1, & 3\nmid n,\\ 0, & 3\mid n;\end{cases} \tag{6}$$

$$\chi(n;3,1)=\begin{cases}1, & n\equiv 1 \pmod 3,\\ -1, & n\equiv 2 \pmod 3,\\ 0, & n\equiv 0 \pmod 3.\end{cases} \tag{7}$$

显见 $\chi(n;3,1)$ 就是 Legendre 符号 $\left(\frac{n}{3}\right)$。同样，模 4 的特征可能的取值是

$$\chi(1;4)=1,$$

及由 $\chi^2(3;4)=\chi(9;4)=\chi(1;4)=1$ 知

$$\chi(3;4)=\pm 1.$$

所以，模 4 的特征也有两个：

$$\chi(n;4,0)=\begin{cases}1, & (n,4)=1,\\ 0, & (n,4)>1;\end{cases} \tag{8}$$

$$\chi(n;4,1)=\begin{cases}1, & n\equiv 1 \pmod 4,\\ -1, & n\equiv 3 \pmod 4,\\ 0, & (n,4)>1.\end{cases} \tag{9}$$

显见，后一个特征就是 $h(n)$，且 $(n,2)=1$ 时，

$$\chi(n;4,1)=\left(\frac{-1}{n}\right)=\left(\frac{-4}{n}\right),$$

$\left(\frac{-1}{n}\right)$, $\left(\frac{-4}{n}\right)$是 Jacobi 符号。

模 5 的特征可能取的值是：

$$\chi(1;5)=1.$$

由 $\chi^4(2;5)=\chi(16;5)=\chi(1;5)=1$ 知

$$\chi(2;5)=e^{2\pi i l/4},\quad l=0,1,2,3.$$

再注意到：$\chi^2(2;5)=\chi(4;5)$，$\chi^3(2;5)=\chi(8;5)=\chi(3;n)$，所以只要 $\chi(2;5)$的取值确定后，其它的取值就确定了，且满足完全积性条件。因此，模 5 的特征有四个，即

$$\chi(n;5,0)=\begin{cases}1, & (n,5)=1,\\ 0, & (n,5)>1;\end{cases}\tag{10}$$

$$\chi(n;5,1)=\begin{cases}1, & n\equiv 1(\bmod 5),\\ i, & n\equiv 2(\bmod 5),\\ -i, & n\equiv 3(\bmod 5),\\ -1, & n\equiv 4(\bmod 5),\\ 0, & n\equiv 0(\bmod 5);\end{cases}\tag{11}$$

$$\chi(n;5,2)=\begin{cases}1, & n\equiv 1(\bmod 5),\\ -1, & n\equiv 2(\bmod 5),\\ -1, & n\equiv 3(\bmod 5),\\ 1, & n\equiv 4(\bmod 5),\\ 0, & n\equiv 0(\bmod 5);\end{cases}\tag{12}$$

$$\chi(n;5,3)=\begin{cases}1, & n\equiv 1(\bmod 5),\\ -i, & n\equiv 2(\bmod 5),\\ i, & n\equiv 3(\bmod 5),\\ -1, & n\equiv 4(\bmod 5),\\ 0. & n\equiv 0(\bmod 5).\end{cases}\tag{13}$$

显见，$\chi(n;5,2)$就是Legendre符号$\left(\frac{n}{5}\right)$.

对给定的模 k，当$(n,k)=1$时，由式(3)知模 k 的特征 $\chi(n)$ 仅能取有限个值，它们是 1 的 $\phi(k)$次单位根

$$e^{2\pi il/\phi(k)},\quad l=0,1,\cdots,\phi(k)-1, \tag{14}$$

所以，对给定的 k，模 k 的特征仅有有限个，我们以$C(k)$表示模 k 的所有不同的特征的个数。上面的例子表明：

$$C(1)=1,\quad C(2)=1,\quad C(3)=2,\quad C(4)=2,\quad C(5)=4.$$

下面将证明：

$$C(k)=\phi(k),\quad k\geqslant 1. \tag{15}$$

显见，当$(n,k)=1$时 $\chi(n)$恒取值 1 的数论函数一定是模 k 的特征，它称为是模 k 的主特征，记作 $\chi^0(n;k)$或 $\chi^0 \bmod k$，即

$$\chi^0(n;k)=\begin{cases}1, & (n,k)=1,\\ 0, & (n,k)>1.\end{cases}$$

模 1 和模 2 仅有一个主特征。一个特征如果它仅取实值，由式(14)知即仅取 ± 1，则称为实特征。主特征一定是实特征，但实特征不一定是主特征。模 3 和模 4 的特征都是实特征，且各有一个是非主特征。一个取到复值的特征称为复特征。模 5 有两个复特征，两个实特征，其中一个是非主特征。

特征有以下基本性质：

性质 1 两个模 k 的特征的乘积是模 k 的特征。

性质 2 若 $\chi(n)$是模 k 的特征，则$\overline{\chi(n)}$也是模 k 的特征（$\bar{\theta}$ 表复数 θ 的共轭数），记作 $\bar{\chi}(n)$，称为特征 $\chi(n)$的共轭特征。当 $nn^{-1}\equiv 1 \pmod k$时，$\bar{\chi}(n)=\chi(n^{-1})$。此外，$\chi\bar{\chi}=\chi^0$，以及当 χ 是实特征时，$\chi=\bar{\chi}$。

性质 3 设 χ,χ_1,χ_2 都是模 k 的特征。若 $\chi\chi_1=\chi\chi_2$，则 $\chi_1=\chi_2$。

性质 4 设模 k 的全部特征是 $\chi_0,\chi_1,\cdots,\chi_h$，$h=C(k)-1$，以及 χ 是任意取定的一个模 k 的特征。那么，

(i) $\bar{\chi}_0,\bar{\chi}_1,\cdots,\bar{\chi}_h$ 也是模 k 的全部特征；

(ii) $\bar{\chi}\chi_0,\bar{\chi}\chi_1,\cdots,\bar{\chi}\chi_h$ 也是模 k 的全部特征。

性质 5 设 $k_1|k_2$。若 k_1 和 k_2 有相同的素因数(即 $p|k_2\Longrightarrow p|k_1$)，则模 k_1 的特征一定是模 k_2 的特征。特别地，当 $l\geqslant d$ 时，模 k^d 的特征一定是模 k^l 的特征。

性质 6 设 χ_1是模k_1的特征，χ_2是模 k_2 的特征。那么，$\chi_1\chi_2$ 是模$[k_1,k_2]$的特征。

这些性质的证明是十分简单的，留给读者。下面的性质是十分重要的。

性质 7 设 $k=k_1k_2,(k_1,k_2)=1,\chi(n;k)$是模 k 的特征。那么，一定存在唯一的模 k_1 的特征 $\chi(n;k_1)$使得

$$\chi(n;k)=\chi(n;k_1),\quad n\equiv 1(\bmod k_2)。\tag{16}$$

证 定义数论函数 $f(m)$如下：对任意整数 m，由孙子定理知，对模 k 存在唯一的 n 满足

$$\begin{cases} n\equiv m(\bmod k_1),\\ n\equiv 1(\bmod k_2)。\end{cases}\tag{17}$$

我们定义

$$f(m)=\chi(n;k)。\tag{18}$$

我们来证明 $f(m)$是模 k_1 的特征。$f(1)=\chi(1;k)=1$，所以 $f(m)$ 不恒为零。若式(17)成立，则必有

$$\begin{cases} n\equiv m+k_1(\bmod k_1),\\ n\equiv 1(\bmod k_2)。\end{cases}$$

因此，$f(m+k_1)=\chi(n;k)=f(m)$。对任意整数 m'，对模 k 存在唯一的 n'满足

$$\begin{cases} n'\equiv m'(\bmod k_1),\\ n'\equiv 1(\bmod k_2)。\end{cases}$$

由此及式(17)得

$$\begin{cases} nn'\equiv mm'(\bmod k_1),\\ nn'\equiv 1(\bmod k_2)。\end{cases}$$

因此，由 χ 的完全积性及 f 的定义知：

$$f(mm') = \chi(nn';k) = \chi(n;k)\chi(n';k)$$
$$= f(m)f(m').$$

这就证明了 f 是完全积性的。最后，当 $(m,k)>1$ 时，由式(17)确定的 n，必有 $(n,k)=(n,k_1)>1$，所以 $f(m)=0$。这就证明了 $f(m)$ 是模 k_1 的特征。现取 $\chi(m;k_1)=f(m)$。当 $m\equiv 1(\bmod k_2)$时，对由式(17)确定的 n，显有 $n\equiv m(\bmod k)$，因此，

$$\chi(m;k_1)=f(m)=\chi(n;k)=\chi(m;k).$$

这就证明了式(16)成立，下面来证唯一性，若还有模 k_1 的特征 $\tilde{\chi}(n;k_1)$满足式(16)，则对任意整数 m，当 n 由式(17)给出时就有

$$\chi(m;k_1)=\chi(n;k_1)=\chi(n;k)=\tilde{\chi}(n;k_1)=\tilde{\chi}(m;k_1).$$

证毕。

定理 1 设 $k=k_1k_2,(k_1,k_2)=1$，$\chi(n;k)$是模 k 的特征。那么，一定存在唯一的一对模 k_1 的特征 $\chi(n;k_1)$及模 k_2 的特征 $\chi(n;k_2)$，使得对任意整数 n 有

$$\chi(n;k)=\chi(n;k_1)\chi(n;k_2). \tag{19}$$

证 先证唯一性。若式(19)成立，则有

$$\chi(n;k)=\chi(n;k_1),\quad n\equiv 1(\bmod k_2), \tag{20}$$
$$\chi(n;k)=\chi(n;k_2),\quad n\equiv 1(\bmod k_1). \tag{21}$$

因而由性质 7 知 $\chi(n;k_1),\chi(n;k_2)$都是唯一的。下证存在性。由性质 7 知，必有模 k_1 的特征 $\chi(n;k_1)$满足式(20)，及模k_2的特征 $\chi(n;k_2)$满足式(21)。对任意整数 n，取

$$\begin{cases} m_1\equiv n(\bmod k_1),\\ m_1\equiv 1(\bmod k_2),\end{cases}$$

及

$$\begin{cases} m_2\equiv 1(\bmod k_1),\\ m_2\equiv n(\bmod k_2).\end{cases}$$

由性质 7 推出：

$$\chi(m_1;k)=\chi(m_1;k_1)=\chi(n;k_1),$$
$$\chi(m_2;k)=\chi(m_2,k_2)=\chi(n;k_2).$$

显见 $m_1m_2\equiv n(\bmod k)$， 由此及完全积性、周期性， 从以上两式即得

$$\chi(n;k)=\chi(m_1m_2;k)=\chi(m_1;k)\chi(m_2;k)$$
$$=\chi(n;k_1)\chi(n;k_2).$$

证毕。

由定理 1 立即推出(证明留给读者)：

推论 2 设 $k=k_1\cdots k_r$，$k_1,\cdots,k_r$ 两两既约，$\chi(n;k)$是模 k 的特征。那么一定存在唯一的一组 r 个特征：模 k_1的特征$\chi(n;k_1)$，$\cdots$，模 k_r 的特征 $\chi(n;k_r)$，使得

$$\chi(n;k)=\chi(n;k_1)\cdots\chi(n;k_r).\tag{22}$$

此外，$\chi(n;k)$是主特征的充要条件是 $\chi(n;k_1),\cdots,\chi(n;k_r)$都是主特征；$\chi(n;k)$是实特征的充要条件是它们都是实特征。特别地，当有素因数分解式

$$k=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}\tag{23}$$

时，有唯一的分解式

$$\chi(n;k)=\chi(n;2^{\alpha_0})\chi(n;p_1^{\alpha_1})\cdots\chi(n;p_s^{\alpha_s}).\tag{24}$$

式(24)表明，为了研究任意模的特征，只要研究模为素数幂的特征。我们先来讨论模 p^α 的特征，素数 $p>2$。设 g 是模p^α 的一个原根(对任意的 $\alpha\geqslant1$，见第五章 § 2定理 3)。 由第五章 § 2 定理 5 及 § 3定义 1 知，对任一$(n,p)=1$ 有

$$n\equiv g^{\gamma(n)}(\bmod p^\alpha),\tag{25}$$

这里 $\gamma(n)$表示以原根 g 为底，n 对模 p^α 的指标， 因而有

$$\chi(n;p^\alpha)=\chi(g^{\gamma(n)};p^\alpha)$$
$$=\{\chi(g;p^\alpha)\}^{\gamma(n)},\quad (n,p)=1.\tag{26}$$

因此，模 p^α 的特征完全由它在原根 g 上的值唯一确定。由式(14)知可能取的值是

$$\chi(g;p^{\alpha})=e^{2\pi i l/\phi(p^{\alpha})},\quad l=0,1,\cdots,\phi(p^{\alpha})-1. \tag{27}$$

所以模 p^{α} 至多有 $\phi(p^{\alpha})$个不同的特征。由指标的性质(见第五章§3性质 2)知，对任意取定的 l，

$$f(n;l)=\begin{cases}e^{2\pi i l\gamma(n)/\phi(p^{\alpha})}, & (n,p)=1,\\ 0, & (n,p)>1\end{cases}$$

一定是模 p^{α} 的特征，且当 $l\not\equiv l'(\bmod\ \phi(p^{\alpha}))$时，$f(g;l)\neq f(g;l')$，所以是不同的特征。此外，当且仅当 $l=0$ 时是主特征，及当且仅当 $l=0,\phi(p^{\alpha})/2$ 时是实特征。这样，我们就证明了

定理 3 设素数 $p>2,\alpha\geqslant1$,及 g 是模 p^{α} 的原根．那么，模 p^{α} 的特征恰有 $\phi(p^{\alpha})$个，它们是

$$\chi(n;p^{\alpha},l)=\begin{cases}e^{2\pi i l\gamma(n)/\phi(p^{\alpha})}, & (n,p)=1,\\ 0, & (n,p)>1,\end{cases}\quad l=0,1,\cdots,\phi(p^{\alpha})-1. \tag{28}$$

例如，对 $k=5$，取原根 $g=2$,式(28)就给出了式(10)—(13)的四个模 5 的特征。

下面来讨论模 2^{α} 的特征．模 2、模 4 的特征前面已经给出(事实上，它们有原根，可像定理3一样讨论)，我们可假定$\alpha\geqslant3$。由于

$$n\equiv(-1)^{\gamma^{(-1)}(n)}5^{\gamma^{(0)}(n)}(\bmod\ 2^{\alpha}), \tag{29}$$

这里 $\gamma^{(-1)}(n),\gamma^{(0)}(n)$是 n 对模 2^{α} 以 $-1,5$ 为底的指标组(见第五章§3定义 2 及第三章§3定理 5)，

$$\gamma^{(-1)}(n)\equiv(n-1)/2\ (\bmod\ 2) \tag{30}$$

(见第五章§3性质 5)，因此，任一模 2^{α} 的特征

$$\begin{aligned}\chi(n;2^{\alpha})&=\chi((-1)^{\gamma^{(-1)}(n)}5^{\gamma^{(0)}(n)};2^{\alpha})\\&=\{\chi(-1;2^{\alpha})\}^{\gamma^{(-1)}(n)}\cdot\{\chi(5;2^{\alpha})\}^{\gamma^{(0)}(n)},\quad(n,2)=1.\end{aligned} \tag{31}$$

因此，模 $2^{\alpha}(\alpha\geqslant3)$的特征 $\chi(n;2^{\alpha})$完全由

$$\chi(-1;2^{\alpha}) \text{ 及 } \chi(5;2^{\alpha})$$

的取值所确定。由于

$$5^{2^{\alpha-2}} \equiv 1 \pmod{2^{\alpha}},$$

所以 $\chi(5;2^{\alpha})$ 仅可能取以下 $2^{\alpha-2}$ 个值：

$$e^{2\pi i l_0/2^{\alpha-2}}, \quad l_0 = 0,1,\cdots,2^{\alpha-2}-1.$$

而 $\chi(-1;2^{\alpha})$ 仅可能取 ± 1 两个值，即

$$e^{2\pi i l_{-1}/2}, \quad l_{-1} = 0,1.$$

所以，模 2^{α} 至多有 $2\cdot 2^{\alpha-2} = \phi(2^{\alpha})$ 个不同的特征。另一方面，由指标组的性质(第五章§3性质6)知，对任意取定的 l_{-1}, l_0，

$$f(n;l_{-1},l_0) = \begin{cases} e^{2\pi i l_{-1}\gamma^{(-1)}(n)/2}\cdot e^{2\pi i l_0 \gamma^{(0)}(n)/2^{\alpha-2}}, & (n,2)=1, \\ 0, & (n,2)>1 \end{cases}$$

一定是模 2^{α} 的特征，且当 $l_{-1} \not\equiv l'_{-1} \pmod 2$ 或 $l_0 \not\equiv l'_0 \pmod{2^{\alpha}}$ 成立时，相应地有

$$f(-1;l_{-1},l_0) \neq f(-1;l'_{-1},l'_0) \text{ 或 } f(5,l_{-1},l_0) \neq f(5;l'_{-1},l'_0)$$

成立，所以是不同的特征。这样就证明了

定理 4 设 $\alpha \geqslant 3$。模 2^{α} 的特征恰有 $\phi(2^{\alpha})$ 个，它们是

$$\chi(n;2^{\alpha},l_{-1},l_0) = \begin{cases} e^{2\pi i l_{-1}\gamma^{(-1)}(n)/2}\cdot e^{2\pi i l_0 \gamma^{(0)}(n)/2^{\alpha-2}}, & (n,2)=1, \\ 0, & (n,2)>1, \end{cases}$$

$$l_{-1} = 0,1, \quad l_0 = 0,1,\cdots,2^{\alpha-2}-1. \tag{32}$$

此外，当且仅当 $l_{-1} = l_0 = 0$ 时是主特征，及当且仅当 $l_0 = 0, 2^{\alpha-3}$ 时是实特征。

这样，综合推论 2 的式(24)、定理 3、定理 4、及模 2、模 4 的特征表达式，就完全解决了模 k(k 由式(23)给出)的特征的构造，因而证明了

定理 5 设 $k \geqslant 1$。模 k 的特征恰有 $\phi(k)$ 个，即式(15)成立。具体的说，若 $k>1$ 的素因数分解式由式(23)给出，$c_{-1} = c_{-1}(\alpha_0), c_0 = c_0(\alpha_0)$ 由第五章§3式(20)给出，$c_j = \phi(p_j^{\alpha_j})$，$g_j$ 是

模$p_j^{\alpha_j}$的原根$(1\leqslant j\leqslant s)$，以及$\gamma^{(-1)}(n),\gamma^{(0)}(n);\gamma^{(1)}(n),\cdots,\gamma^{(s)}(n)$是$n$对模$k$的以$-1,5;g_1,\cdots,g_s$为底的指标组（见第五章§3定义3），那么

$$\chi(n;k)=\chi(n;k,l_{-1},l_0,l_1,\cdots,l_s)$$
$$=\begin{cases}\prod\limits_{j=-1}^{s}e^{2\pi i l_j\gamma^{(j)}(n)/c_j}, & (n,k)=1,\\ 0, & (n,k)>1,\end{cases}\tag{33}$$
$$0\leqslant l_j<c_j,\quad -1\leqslant j\leqslant s$$

恰好给出了模k的全部$\phi(k)$个特征，此外，当且仅当$l_j=0(-1\leqslant j\leqslant s)$时是主特征，以及当且仅当$c_j\mid 2l_j(-1\leqslant j\leqslant s)$时是实特征，即

$$l_j=0\ 或\ l_j=[c_j/2],\quad -1\leqslant j\leqslant s.$$

定理5把$\alpha_0=1$和$\alpha_0=2$的情形也包括了进去，请读者自己写出定理5的详细证明。式(33)给出了模k特征的一个便于研究的表达式。但是由于这里涉及原根和指标组，对它们的性质并不清楚，所以特征的深入研究是十分困难的。

应该指出：由式(33)知，模k的每个特征唯一地对应一组数$\{l_{-1},l_0;l_1,\cdots,l_s\}$；而一组既约剩余系中的每个$n$唯一的对应一组指标组$\{\gamma^{(-1)}(n),\gamma^{(0)}(n);\gamma^{(1)}(n),\cdots,\gamma^{(s)}(n)\}$。$l_j$和$\gamma^{(j)}(n)$的取值范围是相同的，因此，通过关系：

$$l_j=\gamma^{(j)}(n),\quad -1\leqslant j\leqslant s,\tag{34}$$

就可建立模k的全体特征χ和模k的既约剩余系之间的一一对应关系：

$$n\longleftrightarrow\chi \bmod k,\quad (n,k)=1.\tag{35}$$

容易验证（留给读者）：这种对应有性质：设$(n_1,k)=(n_2,k)=1$。若

$$n_1\longleftrightarrow\chi_1 \bmod k,\quad n_2\longleftrightarrow\chi_2 \bmod k,$$

则

$$n_1n_2\longleftrightarrow\chi_1\chi_2 \bmod k.\tag{36}$$

这种对应表明了模k的特征和模k的既约剩余系之间的对偶关

系①。这种对偶关系将在下面的特征性质中显示出来。

由定理 5 推出

定理 6 设 $k>1$，$(a,k)=1$ 及 $a\not\equiv 1(\bmod k)$。那么，一定存在模 k 的一个非主特征 χ，使得 $\chi(a)\neq 1$。

证 设 k 由式(23)给出，并利用定理 5 的符号。由条件知：

$$a\not\equiv 1(\bmod 2^{\alpha_0}),\ a\not\equiv 1(\bmod p_1^{\alpha_1}),\cdots,a\not\equiv 1(\bmod p_s^{\alpha_s})$$

至少有一个成立。若 $a\not\equiv 1(\bmod 2^{\alpha_0})$成立，则 $\gamma^{(-1)}(a),\gamma^{(0)}(a)$一定不全为零。当$0<\gamma^{(-1)}(a)<c_{-1}$时，取$l_{-1}=1,l_0=l_1=\cdots=l_s=0$，特征

$$\chi(n;k)=\chi(n;k,1,0,0,\cdots,0)$$

不是主特征，且(注意这时必有 $\gamma^{(-1)}(a)=1,c_{-1}=2)\chi(a;k)=-1$。当 $0<\gamma^{(0)}(a)<c_0$ 时，取 $l_0=1$，其它 $l_j=0$，则有(这时必有$\alpha_0\geqslant 3$)

$$\chi(a;k,0,1,0,\cdots,0)=e^{2\pi i\gamma^{(0)}(a)/c_0}\neq 1.$$

若 $a\not\equiv 1(\bmod p_i^{\alpha_i})$，则必有 $0<\gamma^{(i)}(a)<c_i$。这时取 $l_i=1$，其它的 $l_j=0$，就有

$$\chi(a;k,0,\cdots,0,1,0,\cdots,0)=e^{2\pi i\gamma^{(i)}(a)/c_i}\neq 1.$$

这就证明了所要的结论。

下面来证明特征的两个重要性质。

定理 7 设 $k\geqslant 1$。我们有

$$\sum_{\chi \bmod k}\chi(n)=\begin{cases}\phi(k), & n\equiv 1(\bmod k),\\ 0, & n\not\equiv 1(\bmod k),\end{cases}\tag{37}$$

这里求和号表示对模 k 的全体特征求和。

证 当 $n\equiv 1(\bmod k)$时，对任一 $\chi \bmod k$ 有 $\chi(n)=1$，因此式(37)左边就是模 k 的特征的个数，由定理 5 知为 $\phi(k)$，这就证明了式(37)的第一式。

当 $n\not\equiv 1(\bmod k)$时，必有 $k>1$。若$(n,k)>1$，则式(37)的第二式显然成立。若$(n,k)=1$，由式(33)知

① 用代数的语言说就是：这两个乘法群是同构的。

$$\sum_{\chi \bmod k} \chi(n) = \sum_{0 \le l_{-1} < c_{-1}} \cdots \sum_{0 \le l_s < c_s} \prod_{j=-1}^{s} e^{2\pi i l_j \gamma^{(j)}(n)/c_j}$$

$$= \left\{ \sum_{0 \le l_{-1} < c_{-1}} e^{2\pi i l_{-1} \gamma^{(-1)}(n)/c_{-1}} \right\} \cdots \left\{ \sum_{0 \le l_s < c_s} e^{2\pi i l_s \gamma^{(s)}(n)/c_s} \right\}.$$

这时必有一个 h， $-1 \le h \le s$，使得 $0 < \gamma^{(h)}(n) < c_h$，因而有

$$\sum_{0 \le l_h < c_h} e^{2\pi i l_h \gamma^{(h)}(n)/c_h} = 0.$$

由以上两式就推出式(37)的第二式这时也成立。证毕。

式(37)的第二式也可以不利用式(33)，而利用定理 6 来证。请读者考虑。

定理 8 设 $k \ge 1$，χ 是一模 k 的特征。我们有

$$\sideset{}{'}\sum_{n \bmod k} \chi(n) = \begin{cases} \phi(k), & \chi = \chi^0 \bmod k, \\ 0, & \chi \ne \chi^0 \bmod k, \end{cases} \tag{38}$$

其中求和号表示对模 k 的一个既约剩余系求和。

证 当 $\chi = \chi^0 \bmod k$ 时，对任意的 $(n,k)=1$ 有 $\chi(n)=1$，这就证明了式(38)的第一式。由定理 5 知，存在一组 $l_{-1}, \cdots, l_s$，使

$$\chi(n) = \chi(n; k, l_{-1}, l_0, \cdots, l_s).$$

当 $\chi \ne \chi^0$ 时，一定有一个 h，$-1 \le h \le s$，使 $0 < l_h < c_h$。由式(33)及第五章 § 3性质 9 知，

$$\sideset{}{'}\sum_{n \bmod k} \chi(n) = \sum_{0 \le \gamma^{(-1)} < c_{-1}} \cdots \sum_{0 \le \gamma^{(s)} < c_s} \prod_{j=-1}^{s} e^{2\pi i l_j \gamma^{(j)}/c_j}$$

$$= \left\{ \sum_{0 \le \gamma^{(-1)} < c_{-1}} e^{2\pi i l_{-1} \gamma^{(-1)}/c_{-1}} \right\} \cdots$$

$$\times \left\{ \sum_{0 \le \gamma^{(s)} < c_s} e^{2\pi i l_s \gamma^{(s)}/c_s} \right\}$$

由此及

$$\sum_{0 \le \gamma^{(h)} < c_h} e^{2\pi i l_h \gamma^{(h)}/c_h} = 0,$$

就推出式(38)的第二式。证毕。

定理 7 与定理 8 从形式到证明都显示了模 k 的既约剩余系和全体特征的对偶关系。同样，式(38)的第二式也可以不利用式(33)，而利用定理 6 来证。请读者考虑。

定理 7 经常利用以下的表示形式：设 $(a,k)=1$。我们有

$$\sum_{\chi \bmod k} \bar{\chi}(a)\chi(n)=\begin{cases}\phi(k), & n\equiv a(\bmod k),\\ 0, & n\not\equiv a(\bmod k).\end{cases} \tag{39}$$

这是因为由 $\bar{\chi}(a)=\chi(a^{-1}),a^{-1}a\equiv 1(\bmod k)$，可推出

$$\sum_{\chi \bmod k} \bar{\chi}(a)\chi(n)=\sum_{\chi \bmod k} \chi(a^{-1}n).$$

由于 $n\equiv a(\bmod k)$ 等价于 $a^{-1}n\equiv 1(\bmod k)$，因而由上式及式(37)就推出式(39)。利用式(39)就可把属于算术数列 $n\equiv a(\bmod k)$ $((a,k)=1)$ 的整数挑选出来。

特征的进一步的性质及其应用超出本书范围。下面仅举几个例子说明数论问题是如何被归结为对特征性质的讨论的。

例 1　设 $x\geqslant 2$，$k>2$，及 $1\leqslant a<k$，$(a,k)=1$。以 $\pi(x;k,a)$ 表算术数列 $n\equiv a(\bmod k)$ 中不超过 x 的素数个数，即

$$\pi(x;k,a)=\sum_{\substack{p\leqslant x\\ p\equiv a(\bmod k)}} 1. \tag{40}$$

在讨论 $\pi(x)$ 时我们可用 $\psi(x)$ 来代替(见第八章§2式(33))。同样的，这里可讨论

$$\psi(x;k,a)=\sum_{\substack{n\leqslant x\\ n\equiv a(\bmod k)}} \Lambda(n). \tag{41}$$

关于 $\pi(x;k,a)$ 和 $\psi(x;k,a)$ 的关系将安排在习题中。利用式(39)可得

$$\pi(x;k,a)=\frac{1}{\phi(k)}\sum_{p\leqslant x}\left\{\sum_{\chi \bmod k} \bar{\chi}(a)\chi(p)\right\}$$

$$=\frac{1}{\phi(k)}\sum_{\chi \bmod k}\bar{\chi}(a)\sum_{p<x}\chi(p)$$

$$=\frac{1}{\phi(k)}\sum_{\substack{p<x\\p\nmid k}}1+\frac{1}{\phi(k)}\sum_{\substack{\chi \bmod k\\ \chi\neq\chi^0}}\bar{\chi}(a)\sum_{p<x}\chi(p), \tag{42}$$

这里的第一项是把相应于模 k 的主特征 χ^0 的一项分出来而得到的。以 $\omega(k,x)$表不超过 x 的 k 的不同的素因数个数，显见 $\omega(k,x)\leqslant\omega(k)$。我们有

$$\pi(x;k,a)=\frac{1}{\phi(k)}\pi(x)-\frac{1}{\phi(k)}\omega(k,x)$$

$$+\frac{1}{\phi(k)}\sum_{\substack{\chi \bmod k\\ \chi\neq\chi^0}}\bar{\chi}(a)\sum_{p<x}\chi(p). \tag{43}$$

一个合理的猜测是：对给定的 $k>2$，素数应"平均地分布在以下 $\phi(k)$ 个算术数列中①：

$$n\equiv a(\bmod k),\quad 1\leqslant a\leqslant k,(a,k)=1. \tag{44}$$

即应有

$$\frac{\pi(x;k,a)}{\pi(x)/\phi(k)}\longrightarrow 1,\quad x\to+\infty. \tag{45}$$

这就是**算术数列中的素数定理**。如果能证明：对每个模 k 的非主特征 χ 有

$$\sum_{p<x}\chi(p)\Big/\pi(x)\longrightarrow 1,\quad x\to+\infty, \tag{46}$$

那么，由此及式(43)就推出式(45)成立。可以证明式(46)成立，但这已超出本书，属于解析数论的内容。这就看出了特征的重要

① 当$(a,k)>1$时，算术数列 $n\equiv a(\bmod k)$中至多有一个素数a，所以不用考虑。

作用，及需要去估计特征和

$$\sum_{p\leqslant x}\chi(p).\tag{47}$$

类似地，可对 $\psi(x;k,a)$进行这样的讨论(见习题 4 第 26题).

例 2 设素数 $p>2$。我们知道在 $1,2,\cdots,p-1$中有一半是模 p 的二次剩余，一半是非剩余。但是，剩余和非剩余的分布很不规则。一个著名的数论问题是求模 p 的正的最小的二次非剩余 $n(p)$。显见，若存在整数 $A,1<A\leqslant(p+1)/2$，使得

$$\sum_{a=1}^{A}\left(\frac{a}{p}\right)<A,\tag{48}$$

则 $n(p)\leqslant A$，这里 Legendre 符号是模 p 的实特征。在习题四第22题中将给出一个形如式(48)的估计。

以上两个例子表明需要讨论特征和

$$\sum_{a<n\leqslant b}f(n)\chi(n)\tag{49}$$

的性质，特别是它的上界估计，这里 $f(n)$是某个数论函数。

例 3 设 p 是素数，$r\geqslant1$，及 a 是一整数。以$T(r;a)$ 表示同余方程

$$x_1^2+\cdots+x_r^2\equiv a(\mathrm{mod}\ p)$$

的解数。当 $r=1$ 时，已知

$$T(1;a)=1+\left(\frac{a}{p}\right).\tag{50}$$

下面我们来看当 $r\geqslant2$ 时应如何求 $T(r;a)$。我们有

$$T(r;a)=\frac{1}{p}\sum_{l=1}^{p}\sum_{x_1=1}^{p}\cdots\sum_{x_r=1}^{p}e^{2\pi il(x_1^2+\cdots+x_r^2-a)/p}$$

$$=\frac{1}{p}\sum_{l=1}^{p}e^{-2\pi ial/p}\left\{\sum_{x=1}^{p}e^{2\pi ilx^2/p}\right\}^r.$$

由式(50)知

$$\sum_{x=1}^{p} e^{2\pi i l x^2/p} = \sum_{y=1}^{p}\left(1+\left(\frac{y}{p}\right)\right)e^{2\pi i l y/p}.$$

进而有

$$T(r,a)=\frac{1}{p}\sum_{l=1}^{p}e^{-2\pi i a l/p}\left\{\sum_{y=1}^{p}e^{2\pi i l y/p}+\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i l y/p}\right\}^r$$

$$=p^{r-1}+\frac{1}{p}\sum_{l=1}^{p-1}e^{-2\pi i a l/p}\left\{\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i l y/p}\right\}^r.$$

这里用到了 $\sum_{y=1}^{p}\left(\frac{y}{p}\right)=0$。当 $(l,p)=1$ 时，$\left(\frac{l}{p}\right)^2=1$，及 y 和 ly 同时遍历模 p 的完全剩余系，所以

$$\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i l y/p}=\left(\frac{l}{p}\right)\sum_{y=1}^{p}\left(\frac{ly}{p}\right)e^{2\pi i l y/p}$$

$$=\left(\frac{l}{p}\right)\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}.$$

因而

$$T(r;a)=\begin{cases} p^{r-1}+\frac{1}{p}\left\{\sum_{l=1}^{p-1}e^{-2\pi i a l/p}\right\}\left\{\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}\right\}^r, & 2\mid r;\\ p^{r-1}+\frac{1}{p}\left\{\sum_{l=1}^{p-1}\left(\frac{l}{p}\right)e^{-2\pi i a l/p}\right\} \\ \qquad\cdot\left\{\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}\right\}^r, & 2\nmid r. \end{cases}$$

当 $p\mid a$ 时，

$$T(r;a)=\begin{cases} p^{r-1}+\left(1-\frac{1}{p}\right)\left\{\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}\right\}^r, & 2\mid r,\\ p^{r-1}, & 2\nmid r. \end{cases} \tag{51}$$

当 $p\nmid a$ 时，

$$\sum_{l=1}^{p-1} e^{-2\pi i a l/p} = -1,$$

$$\sum_{l=1}^{p-1}\left(\frac{l}{p}\right)e^{-2\pi i a l/p} = \left(\frac{-a}{p}\right)\sum_{l=1}^{p-1}\left(\frac{-al}{p}\right)e^{-2\pi i a l/p}$$

$$= \left(\frac{-a}{p}\right)\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p},$$

这里用到了$p\nmid a$时$\left(\frac{-a}{p}\right)^2=1$，及$-al$和 l 同时遍历模 p 的既约剩余系。因此，当$p\nmid a$时，

$$T(r;a)=\begin{cases} p^{r-1}-\dfrac{1}{p}\left\{\displaystyle\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}\right\}^r, & 2\mid r, \\ p^{r-1}+\dfrac{1}{p}\left(\dfrac{-a}{p}\right)\left\{\displaystyle\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}\right\}^{r+1}, & 2\nmid r. \end{cases} \tag{52}$$

因此，为了求$T(r;a)$导致讨论

$$\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}. \tag{53}$$

可以证明(见[2]，第七章§5)：对奇素数 p 有

$$\sum_{y=1}^{p}\left(\frac{y}{p}\right)e^{2\pi i y/p}=\begin{cases}\sqrt{p}, & p\equiv 1 \pmod 4, \\ i\sqrt{p}, & p\equiv -1 \pmod 4.\end{cases} \tag{54}$$

由此即得：当$p\mid a$时，

$$T(r;a)=\begin{cases} p^{r-1}+(p-1)p^{r/2-1}, & 2\mid r,\ p\equiv 1 \pmod 4, \\ p^{r-1}+(-1)^{r/2}(p-1)p^{r/2-1}, & 2\mid r,\ p\equiv 3 \pmod 4, \\ p^{r-1}, & 2\nmid r. \end{cases} \tag{55}$$

当$p\nmid a$时，

$$T(r;a)=\begin{cases} p^{r-1}-p^{r/2-1}, & 2\mid r,\ p\equiv 1 \pmod 4, \\ p^{r-1}-(-1)^{r/2}p^{r/2-1}, & 2\mid r,\ p\equiv 3 \pmod 4, \end{cases} \tag{56}$$

及

$$T(r;a)=\begin{cases} p^{r-1}+\left(\frac{a}{p}\right)p^{(r-1)/2}, \\ \qquad 2\nmid r,\quad p\equiv 1 \pmod 4, \\ p^{r-1}-\left(\frac{a}{p}\right)(-1)^{(r+1)/2}p^{(r-1)/2}, \\ \qquad 2\nmid r,\quad p\equiv 3 \pmod 4, \end{cases} \tag{57}$$

这里用到了$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$. 显见，以上各式当$r=1$时也成立。

这个例子表明型如式(53)的特征和在数论中的重要作用。更一般地对模k的特征χ，可考虑特征和

$$G(a;\chi)=\sum_{l=1}^{k}\chi(l)e^{2\pi ial/k}, \tag{58}$$

a为一整数。$G(a;\chi)$通常称为关于特征χ的Gauss和。

习 题 四

1. 写出模$k=6,7,8,9,11,13,15,20$的全体特征，并指出它们的非主实特征。

2. 模k的特征$\chi(n;k)$可用以下方法来定义：

(i) $\chi(n;1)=1$;

(ii) 对奇素数p及$\alpha\geqslant1$，$\chi(n;p^{\alpha})$由§4式(28)定义；

(iii) $\chi(n;2^{\alpha})$由§4式(5),(8),(9)及(31)定义；

(iv) 一般的$\chi(n;k)$由§4式(33)定义。

证明：这样的定义和§4定义1是等价的，并由这里的定义也可直接推出特征的所有性质。

3. 设$k=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. 证明：$\chi(n;k)$是实特征的充要条件是：

(i) 当 $a_0=0$时，$\chi(n;k)=\left(\frac{n}{p_1}\right)^{\beta_1}\cdots\left(\frac{n}{p_s}\right)^{\beta_s}$，这里$\beta_j=1$或2；

(ii) 当$a_0\geqslant1$时，

$$\chi(n;k)=\left(\frac{-4}{n}\right)^{\beta_{-1}}\left(\frac{8}{n}\right)^{\beta_0}\left(\frac{n}{p_1}\right)^{\beta_1}\cdots\left(\frac{n}{p_s}\right)^{\beta_s},$$

这里$\beta_j=1$或 2，$2\nmid n$。

4．数论函数$f(n)$称为是周期的，如果存在正整数q，使对任意整数n有$f(n+q)=f(n)$。设$f(n)$是周期的。证明：(i) 若q_0是具有上述性质的q中的最小的，则$q_0|q$。q_0称为$f(n)$的最小正周期；(ii) 若$f(n)$是完全积性的且不恒为零，则$f(n)$一定是模q_0的特征。

5．当$\mu(k)\neq0$时，$\chi(n;k)$的最小正周期(见上题)为k。

6．(i) 如何确定由式(28)给出的$\chi(n;p^a)$的最小正周期；(ii) 如何确定由式(31)给出的$\chi(n;2^a)$的最小正周期；(iii) 设$\chi(n;k)$由式(24)给出，证明：它的最小正周期等于右边各个特征的最小正周期的乘积。

7．特征$\chi(n;k)$称为是**模k的非原特征**，如果存在正整数$k'<k$，使对任意的$(n_1n_2,k)=1$，当$n_1\equiv n_2 \pmod{k'}$时，必有$\chi(n_1;k)=\chi(n_2;k)$。不然，$\chi(n;k)$就称为是**模k的原特征**。证明：

(i) 若$\chi(n;k)$是非原特征，记满足定义要求的最小的k'为k^*，则必有$k^*|k$；

(ii) 非原特征的定义等价于：存在正整数$k'<k$，使对任意的$(n,k)=1$，当$n\equiv1 \pmod{k'}$时，必有$\chi(n;k)=1$。

8．证明：(i) 模 1 的特征是原特征；(ii) 模 2 没有原特征；(iii) $\chi(n;4,0)$(见式(8))不是原特征，$\chi(n;4,1)$(见式(9))是原特征；(iv) $\chi(n;p^a,l)$(见式(28))是原特征的充要条件是$(l,p)=1$；(v) $\chi(n;2^a,l_{-1},l_0)$($a\geqslant3$，见式(32))是原特征的充

要条件是$2\nmid l_0$。(vi) 若$\chi(n;k)$有式(22)或式(24)成立，则$\chi(n;k)$是(实)原特征的充要条件是式(22)或式(24)右边的各个特征都是(实)原特征。

9．以$P(k)$表示模k的原特征的个数，(i) 证明$P(k)$是k的积性函数；(ii) $\sum_{d\mid k}P(d)=\phi(k)$；(iii) 求$P(p^{\alpha})$的值，$p$为素数。

10．设p是素数，$k=p^{\alpha}$，$\alpha\geqslant1$，证明：当且仅当$k=4,8$及奇素数p时，模k有实原特征存在。它们是$\chi(n;4,1)$(见式(9))，$\chi(n;8,0,1)$，$\chi(n;8,1,1)=\chi(n;4,1)\chi(n;8,0,1)$(见式(32))，及$\chi(n;p,(p-1)/2)=\left(\frac{n}{p}\right)$，$p$为奇素数(见式(28))。

11．设p为素数，$\alpha\geqslant1$，证明：

(i) 对取定的p，模$p^{\alpha}(\alpha\geqslant1)$的主特征都相同；

(ii) 对模p^{α}的每一个非主特征，必有唯一的模$k^*=p^{\lambda}$，$1\leqslant\lambda\leqslant\alpha$，及模$k^*$的唯一的一个原特征与它恒等；

(iii) 对取定的$\alpha\geqslant1$，对模$p^{\lambda}(1\leqslant\lambda\leqslant\alpha)$的每一个特征，必有唯一的一个模$p^{\alpha}$的特征与它恒等。

12．对模k的每一个特征$\chi(n;k)$，一定存在唯一的模k^*，$k^*\mid k$，及模k^*的唯一的原特征$\chi^*(n;k^*)$，使当$(n,k)=1$时必有$\chi(n;k)=\chi^*(n;k^*)$。反过来，对每个$k^*\mid k$，及模k^*的每一个原特征$\chi^*(n;k^*)$，一定存在模k的唯一的特征$\chi(n;k)$，使当$(n,k)=1$时，$\chi(n;k)=\chi^*(n;k^*)$。事实上，我们有$\chi(n;k)=\chi^*(n;k^*)\cdot\chi^0(n;k)$，$\chi^0(n;k)$是模$k$的主特征。

13．当$k=p^{\alpha}$，$\chi(n;k)$不是主特征时，上题中的k^*就是$\chi(n;k)$的最小正周期(见第4题)，举例说明，当k不是素数幂时这结论不成立。

14．模k的所有特征都是实特征的充要条件是$k=1,2,3,4,6,8,12$，或24。

15．设$f(n)$是周期为k的数论函数，记$e(\theta)=e^{2\pi i\theta}$．证明：

$f(n)=\sum_{l=1}^{k}a_l e(-nl/k)$，这里 $a_l=(1/k)\sum_{m=1}^{k}f(m)e(lm/k)$。特别的，当取 $f(n)=\chi(n;k)$ 时，$a_l=(1/k)G(l;\chi)$，这里 $G(l;\chi)$ 由式(58)给出。

16．设 $G(a;\chi)$ 由式(58)给出。证明：

(i) 当 $a_1\equiv a_2(\bmod k)$ 时，$G(a_1;\chi)=G(a_2;\chi)$；

(ii) $G(-a;\chi)=\chi(-1)G(a;\chi)$；

(iii) $G(a;\bar{\chi})=\chi(-1)\overline{G(a;\chi)}$；

(iv) $G(0;\chi)=\phi(k)$，当 $\chi=\chi^0$；$G(0;\chi)=0$，当 $\chi\neq\chi^0$；

(v) 当 $(a,k)=1$ 时，$G(a;\chi)=\bar{\chi}(a)G(1,\chi)$；

(vi) 在§4 定理 1 的条件和符号下，记 $\chi=\chi(n;k)$，$\chi_1=\chi(n;k_1)$，$\chi_2=\chi(n;k_2)$，我们有

$$G(a;\chi)=\chi_1(k_2)\chi_2(k_1)G(a;\chi_1)G(a;\chi_2)；$$

(vii) 当 $(a,k)=1$ 时，$G(a;\chi^0)=\mu(k)$，χ^0 是模 k 的主特征；一般的有

$$G(a;\chi^0)=\mu(k/(k,a))\phi(k)/\phi(k/(k,a)),$$

$G(a;\chi^0)$ 是 k 的积性函数。

17．设 $G(a;\chi)$ 由式(58)给出，χ 是模 k 的原特征，及 $(a,k)=\lambda>1$。记 $a=\lambda a'$，$k=\lambda k'$。证明：

(i) $G(a;\chi)=\sum_{n=1}^{k'}S(n)e(a'n/k')$，其中 $e(\theta)=e^{2\pi i\theta}$，

$$S(n)=\sum_{l=0}^{\lambda-1}\chi(n+k'l)；$$

(ii) 当 $n_1\equiv n_2(\bmod k')$ 时，$S(n_1)=S(n_2)$；

(iii) 由 χ 是模 k 的原特征推出 $S(n)\equiv0$；

(iv) $G(a;\chi)=0$。

18．(i) 当 χ 是模 k 的原特征时，总有 $G(a;\chi)=\bar{\chi}(a)G(1;\chi)$；

(ii) 当 χ 是模 k 的原特征时，$|G(1;\chi)|=\sqrt{k}$；

(iii) 当χ是模k的实原特征时，$G^2(1,\chi)=\chi(-1)k$；

(iv) 当χ是模 p 的 Legendre 符号时，$G(1,\chi)=\pm\sqrt{p}$，$p\equiv 1(\bmod 4)$；$G(1,\chi)=\pm i\sqrt{p}$，$p\equiv 3(\bmod 4)$。

19．设χ是模k的特征，χ^*是第12题中所确定的对应于χ的模k^*的原特征。证明：

$$G(1;\chi)=\chi^*(k/k^*)\mu(k/k^*)G(1;\chi^*).$$

20．设$k\geqslant 3$，χ是模k的原特征。利用第18题证明：对任意整数M及正整数N，有

$$\left|\sum_{n=M+1}^{M+N}\chi(n)\right|\leqslant\frac{1}{\sqrt{k}}\sum_{l=1}^{k-1}\left(\sin\frac{\pi l}{k}\right)^{-1}.$$

进而推出

$$\left|\sum_{n=M+1}^{M+N}\chi(n)\right|<\sqrt{k}\ln k.$$

21．利用第12,20题推出：对任意整数M及正整数N，当χ是模 k 的非主特征时，有 $\left|\sum_{n=M+1}^{M+N}\chi(n)\right|<2\sqrt{k}\ln k$。

22．设 p 为奇素数。证明：模 p 的正的最小二次非剩余不大于$[\sqrt{p}\ln p]+1$。

23．设 p 是奇素数，N_p 表模 p 的正的最小二次非剩余，及$N(x)$表不超过 x 的模 p 的正的二次非剩余的个数。证明：

(i) 若 a 是模 p 的正的二次非剩余，则必有素数 $q|a$，$q\geqslant N_p$，q 是模 p 的二次非剩余；

(ii) 对任意的 $1<y<N_p<x$ 有 $N(x)\leqslant\sum_{y<q\leqslant x}\left[\frac{x}{q}\right]$，这里 q 是素变数；

(iii) $N(x)>[x]/2-(\sqrt{p}\ln p)/2$；

(iv) 取 $x=\sqrt{p}\ln^2 p$。若$N_p\geqslant p^\delta\ln^2 p$，$\delta=(2\sqrt{e})^{-1}$，利用§3定理11，从(ii)及(iii)推出矛盾。所以对充分大的 p 有 $N_p<p^\delta\ln^2 p$ 成立。

24．设χ是模k的非主特征．证明：

(i) 当 $s>0$时，级数$\sum_{n=1}^{\infty}\chi(n)n^{-s}$收敛，且当$s>1$时，

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_{p}\left(1-\frac{\chi(p)}{p^{s}}\right)^{-1};$$

(ii) 当$s>1$时

$$L^{-1}(s,\chi)=\sum_{n=1}^{\infty}\mu(n)\chi(n)n^{-s};$$

(iii) 当 $s>1$时，

$$\ln L(s,\chi)=\sum_{n=2}^{\infty}\Lambda(n)\chi(n)(\ln n)^{-1}n^{-s};$$

(iv) 当$s>1$时，

$$-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{n=1}^{\infty}\Lambda(n)\chi(n)n^{-s}.$$

25．设$x\geqslant 2$，$(a,k)=1$，$1\leqslant a\leqslant k$．证明：

(i)

$$\psi(x;k,a)=\sum_{\substack{n\leqslant x\\ n\equiv a(\bmod k)}}\Lambda(n)$$

$$=\frac{1}{\phi(k)}\sum_{\chi \bmod k}\overline{\chi}(a)\psi(x,\chi),$$

这里

$$\psi(x;\chi)=\sum_{n\leqslant x}\Lambda(n)\chi(n);$$

(ii)

$$\psi(x;k,a)=\frac{1}{\phi(k)}\psi(x)+\frac{1}{\phi(k)}\sum_{\substack{\chi \bmod k\\ \chi\neq\chi^{0}}}\overline{\chi}(a)\psi(x;\chi)$$

$$-r(x,k),$$

这里

$$0\leqslant r(x,k)<\frac{1}{\phi(k)}\omega(k)\ln x.$$

26. 设 p 为奇素数，以$T_p^*(r)$表同余方程

$$x_1^2+\cdots+x_r^2\equiv 0(\bmod p),\qquad 1\leqslant x_1<\cdots<x_r\leqslant(p-1)/2$$

的解数。证明：

(i) $T_p^*(2)=(p-1)/4$，当 $p\equiv 1(\bmod 4)$；$T_p^*(2)=0$，当 $p\equiv 3(\bmod 4)$；

(ii) $T_p^*(3)=T_5^*(3)=0$。当$p>5$时有

$$\begin{aligned}(3!)pT_p^*(3)=&\sum_{l=1}^{p}\sum_{x_1=1}^{c}\sum_{x_2=1}^{c}\sum_{x_3=1}^{c}e^{2\pi il(x_1^2+x_2^2+x_3^2)/p}\\&-3\sum_{l=1}^{p}\sum_{x_1=1}^{c}\sum_{x_2=1}^{c}e^{2\pi il(x_1^2+2x_2^2)/p}\\&+2\sum_{l=1}^{p}\sum_{x_1=1}^{c}e^{2\pi il(3x_1^2)/p},\end{aligned}$$

其中$c=(p-1)/2$。这公式当$p=3,5$时也成立；

(iii) $T_3^*(4)=T_5^*(4)=T_7^*(4)=0$。当$p>7$时，

$$\begin{aligned}(4!)pT_p^*(4)=&\sum_{l=1}^{p}\sum_{x_1=1}^{c}\cdots\sum_{x_4=1}^{c}e^{2\pi il(x_1^2+\cdots+x_4^2)/p}\\&-6\sum_{l=1}^{p}\sum_{x_1=1}^{c}\sum_{x_2=1}^{c}\sum_{x_3=1}^{c}e^{2\pi il(x_1^2+x_2^2+2x_3^2)/p}\\&+3\sum_{l=1}^{p}\sum_{x_1=1}^{c}\sum_{x_2=1}^{c}e^{2\pi il(2x_1^2+2x_2^2)/p}\\&+8\sum_{l=1}^{p}\sum_{x_1=1}^{c}\sum_{x_2=1}^{c}e^{2\pi il(x_1^2+3x_2^2)/p}.\end{aligned}$$

这公式当$p=3,5,7$时也成立；

(iv) 利用§4例3的方法及式(54)，求 $T_p^*(3)$及$T_p^*(4)$的表达式。

附录一　自　然　数

§1　Peano 公 理

自然数，也叫作**正整数**，就是大家所熟知的

$$1,2,3,\cdots,n,\cdots。\qquad (1)$$

它的形成和我们对它性质的认识都源于经验。自然数集合严格的抽象定义是由 Peano 公理给出的，它刻画了自然数的本质属性，并导出有关自然数的所有运算和性质。下面我们来给出这一公理化定义。

Peano公理　设$\boldsymbol{N}$是一个非空集合，满足以下条件：

(i) 对每一个元素$n\in\boldsymbol{N}$，一定有唯一的一个$\boldsymbol{N}$中的元素与之对应，这个元素记作n^+，称为是n的**后继元素**(或**后继**)；

(ii) 有元素$e\in\boldsymbol{N}$，它不是$\boldsymbol{N}$中任一元素的后继；

(iii) $\boldsymbol{N}$中的任意一个元素至多是一个元素的后继，即从$a^+=b^+$一定可推出$a=b$；

(iv) (归纳公理) 设S是$\boldsymbol{N}$的一个子集合，$e\in S$。如果$n\in S$，则必有$n^+\in S$。那么，$S=\boldsymbol{N}$。

这样的集合$\boldsymbol{N}$称为**自然数集合**，它的元素叫作自然数。

由定义立即可推出自然数集合有以下性质。

定理1　对任意的$n\in\boldsymbol{N}$有$n\neq n^+$。

证　$\boldsymbol{N}$中所有使得$n\neq n^+$成立的元素n组成的子集记作S。由公理(ii)知$e\neq e^+$，所以$e\in S$，S为非空。若$n\in S$，即$n\neq n^+$，我们来证明必有$n^+\in S$。因若不然，则有$n^+=(n^+)^+$，由此及公理(iii)推出$n=n^+$，矛盾。因而由归纳公理推出$S=\boldsymbol{N}$。证毕。

定理2　设$m\in\boldsymbol{N}$，$m\neq e$，那么，必有$n\in\boldsymbol{N}$使得$n^+=m$，即

N中每个不等于e的元素必是某个元素的后继，e是唯一没有后继的元素。此外，这个元素n是唯一的，记作m^-，称为是m的**前导元素**（或前导）。

证 设集合A由N中所有这样的元素a组成：a必是某个元素的后继。因为有$e^+ \in A$，所以A非空。设并集$S=\{e\}\cup A$。显见，$e\in S$。若$n\in S$，由A的定义知$n^+\in A$，因而$n^+\in S$。由归纳公理(iv)就推出$S=N$。因此，若$m\in N$，$m\neq e$就必有$m\in A$。这就证明了定理的前半部分。由公理(iii)就推出定理的后半部分。

以上两个定理的证明方法实际上就是通常所说的归纳法，它基于归纳公理(iv)。一般的可表述为

定理3（归纳证明原理） 设$P(n)$是关于自然数n的一种性质或命题。如果当$n=e$时，$P(e)$成立，以及由$P(n)$成立必可推出$P(n^+)$成立，那么，$P(n)$对所有的$n\in N$都成立。

证 设S是使$P(n)$成立的所有n组成的集合。由条件知$e\in S$，且当$n\in S$时必有$n^+\in S$。因而由归纳公理(iv)知定理成立。证毕。

为了说明我们所十分熟悉的自然数(1)就是由Peano公理所定义的抽象自然数集合的一个具体模型，就需要在抽象自然数集合N中相应的引入“加法”、“乘法”运算，“大小”（即“顺序”）的概念，以及证明它们满足熟知的性质。这就是下面几节的内容。为此，这里先引进集合上的二元运算的概念。

二元运算 设X是一个集合，它的有序对组成的集合，即乘积集合$X\cdot X$是

$$Y=X\cdot X=\{\{a,b\}:\ a\in X,b\in X\}. \tag{2}$$

从集合Y到集合X的一个映射τ就称为是X上的一个二元运算。也就是说，对任意两个元素$a,b\in X$，有序对$\{a,b\}$按规律τ对应于X的一个唯一确定的元素，记作$\tau\{a,b\}$，或$a\tau b$。二元运算τ称为是**结合的**，如果对任意的$a,b,c\in X$有

$$(a\tau b)\tau c=a\tau(b\tau c); \tag{3}$$

二元运算τ称为是交换的，如果对任意的$a,b\in X$有

$$a\tau b=b\tau a. \qquad (4)$$

§2 加法与乘法

本节来定义自然数集合$\boldsymbol{N}$上的加法运算与乘法运算，并给出它们所满足的性质。

定理1 在自然数集合$\boldsymbol{N}$上一定存在唯一的一个二元运算σ，满足条件：

(i) 对任意的$n\in\boldsymbol{N}$有

$$n\sigma e=n^{+}; \qquad (1)$$

(ii) 对任意的$n,m\in\boldsymbol{N}$有

$$n\sigma m^{+}=(n\sigma m)^{+}. \qquad (2)$$

先来证明一个引理。

引理2 对任意给定的$n\in\boldsymbol{N}$，一定存在唯一的一个$\boldsymbol{N}$到其自身的映射f_n，满足

$$f_n(e)=n^{+}; \qquad (3)$$

以及对任意的$m\in\boldsymbol{N}$有

$$f_n(m^{+})=(f_n(m))^{+}. \qquad (4)$$

证 先证唯一性。若还存在一个这样的映射g_n，则当$m=e$时，由(3)得$g_n(e)=f_n(e)=n^{+}$。假设对某个$m\in\boldsymbol{N}$有$g_n(m)=f_n(m)$，那么由(4)得

$$g_n(m^{+})=(g_n(m))^{+}=(f_n(m))^{+}=f_n(m^{+}).$$

因此，由§1定理3（归纳证明原理）知，对一切$m\in\boldsymbol{N}$有$g_n(m)=f_n(m)$。这就证明了唯一性，下面来证存在性。当$n=e$时，我们定义$\boldsymbol{N}$到自身的映射

$$f_e(m)=m^{+}, \qquad m\in\boldsymbol{N}, \qquad (5)$$

就满足要求。因为$f_e(e)=e^{+}$，所以条件(3)满足。对任意的$m\in\boldsymbol{N}$，由定义(5)得

$$f_e(m^+)=(m^+)^+=(f_e(m))^+,$$

即条件(4)满足。假设对 n 存在这样的映射 f_n，对n^+定义$\boldsymbol{N}$到自身的映射

$$f_{n^+}(m)=(f_n(m))^+,\qquad m\in\boldsymbol{N},\tag{6}$$

由此及映射f_n满足条件(3)与(4)，就推出

$$f_{n^+}(e)=(f_n(e))^+=(n^+)^+,$$

$$f_{n^+}(m^+)=(f_n(m^+))^+=((f_n(m))^+)^+=(f_{n^+}(m))^+,$$

这就证明了映射f_{n^+}满足条件(3)与(4)。因此，由归纳证明原理(§1定理3)就证明了对任意的$n\in\boldsymbol{N}$一定存在满足条件(3)与(4)的映射f_n。证毕。

定理1的证明 先证存在性。对任一$n\in\boldsymbol{N}$，设f_n是引理2中确定的映射。现定义二元运算σ：

$$n\sigma m=f_n(m),\qquad n\in\boldsymbol{N},\ m\in\boldsymbol{N}.\tag{7}$$

由式(3)得

$$n\sigma e=f_n(e)=n^+,$$

所以条件(1)满足；由式(4)得

$$n\sigma m^+=f_n(m^+)=(f_n(m))^+=(n\sigma m)^+,$$

所以条件(2)成立。因此，由式(7)定义的二元运算满足定理要求。再证唯一性。设还有二元运算η也满足(1)与(2)。当$m=e$时，对所有的$n\in\boldsymbol{N}$有

$$n\sigma e=n^+=n\eta e.$$

若对某个m，对任意的$n\in\boldsymbol{N}$，有$n\sigma m=n\eta m$，那么，对m^+及任意的$n\in\boldsymbol{N}$有

$$n\sigma m^+=(n\sigma m)^+=(n\eta m)^+=n\eta m^+.$$

所以，由归纳证明原理知，对任意的$n\in\boldsymbol{N}$及$m\in\boldsymbol{N}$有

$$n\sigma m=n\eta m.$$

这就证明了唯一性。

基于定理1就可以定义加法。

加法 我们把满足定理 1 的二元运算σ称为是**自然数集合 $\boldsymbol{N}$ 上的加法运算（或加法）**，并记作

$$n\sigma m = n + m, \qquad n, m \in \boldsymbol{N}.$$

下面来证明加法运算所满足的规律及性质。

(1) **加法结合律** 对任意的 $a, b, c \in \boldsymbol{N}$ 有

$$(a+b)+c = a+(b+c). \tag{8}$$

证 当$c = e$时，对任意的$a, b \in \boldsymbol{N}$，由式(1)和(2)得

$$(a+b)+e = (a+b)^+ = a+b^+ = a+(b+e),$$

所以式(8)成立。假设式(8)对某个$c = n$及任意的 $a, b \in \boldsymbol{N}$ 成立。当$c = n^+$，对任意的$a, b \in \boldsymbol{N}$就有（利用式(2)及假设）

$$(a+b)+n^+ = ((a+b)+n)^+ = (a+(b+n))^+$$
$$= a+(b+n)^+ = a+(b+n^+),$$

即式(8)对$c = n^+$及任意的 $a, b \in \boldsymbol{N}$ 也成立。由归纳证明原理就证明了结论。

(2) **加法交换律** 对任意的$a, b \in \boldsymbol{N}$有

$$a+b = b+a. \tag{9}$$

证 先证对任意的 $b \in \boldsymbol{N}$ 有

$$e+b = b+e. \tag{10}$$

当$b = e$时式(10)显然成立。假设$b = n$时式(10)成立。当$b = n^+$时，由式(2)，假设，及式(1)得

$$e+n^+ = (e+n)^+ = (n+e)^+ = (n^+)^+ = n^+ + e,$$

即式(10)也成立。因此，由归纳证明原理知式(10)成立。

式(10)表明式(9)当$a = e$时，对任意的$b \in \boldsymbol{N}$成立。假设式(9)当$a = n$时，对任意的$b \in \boldsymbol{N}$成立。当 $a = n^+$ 时，对任意的 $b \in \boldsymbol{N}$，利用式(1)，(8)，(10)，(2)及假设可得

$$n^+ + b = (n+e)+b = n+(e+b) = n+(b+e)$$
$$= n+b^+ = (n+b)^+ = (b+n)^+ = b+n^+,$$

即式(9)也成立。所以由归纳证明原理就证明了所要结论。

(3) **加法相消律** 设$a, b, c \in \boldsymbol{N}$。若$b+a = c+a$，则$b = c$。

证 先证结论当$a=e$时成立．若有$b+e=c+e$．由式(1)知$b+e=b^+$，$c+e=c^+$，所以$b^+=c^+$．由Peano公理(iii)就推出$b=c$，所以当$a=e$时成立．假设$a=n$时成立．当$a=n^+$时，若有$b+n^+=c+n^+$，则由式(2)知

$$(b+n)^+=(c+n)^+.$$

由此从Peano公理(iii)知$b+n=c+n$，进而由假设知$b=c$，即结论对$a=n^+$也成立，因此，由归纳证明原理就证明了所要结论．

(4) 对任意的$a,b\in N$有$b+a\neq a$．

证 当$a=e$时，$b+e=b^+$，由此及Peano公理(ii)知$b+e\neq e$成立．假设$a=n$时，结论成立，当$a=n^+$时，由式(4)知

$$b+n^+=(b+n)^+.$$

若$b+n^+=n^+$，则由Peano公理(iii)将推出$b+n=n$，这和假设矛盾．所以也有$b+n^+\neq n^+$．因而由归纳证明原理就推出所要结论．

(5) 对任意的$a,b\in N$，以下三种情形有且仅有一种成立：(i) $a=b$；(ii) 存在$x\in N$使得$a=b+x$；(iii) 存在$y\in N$使得$a+y=b$．

证 当$b=e$时，结论成立．因为，若$a=e$则有(i)成立；若$a\neq e$，由§1定理2知$a=(a^-)^+$，进而由式(1)及交换律得$a=a^-+e=e+a^-$，即有(ii)成立。此外，由性质(4)容易推出：对任意的a和b这三种情形至多只能有一种成立．假设$b=n$时结论成立．当$b=n^+$时，若$a=e$，则$n^+=e+n$，所以有(iii)成立；若$a\neq e$，则由§1定理2知$a=(a^-)^+$．由假设知对a^-和n这三种情形必有一成立．若$a^-=n$，则推出$a=n^+$，所以情形(i)成立；若$a^-=n+x=x+n$，那末，$a=(a^-)^+=(x+n)^+=x+n^+=n^++x$，所以情形(ii)成立，这里用到了式(4)和交换律；同样，从$a^-+y=n$可推出$a+y=n^+$，即有情形(iii)成立．所以，结论对$b=n^+$也成立．由归纳证明原理就推出所要结论．

为了定义乘法运算，先来证明

定理3 在自然数集合N上一定存在唯一的一个二元运算π，满足条件：

(i) 对任意的$n \in N$有

$$n\pi e = n; \tag{11}$$

(ii) 对任意的$n, m \in N$有

$$n\pi m^{+} = (n\pi m) + n. \tag{12}$$

为此先证一个引理。

引理4 对任意给定的$n \in N$，一定存在唯一的一个N到自身的映射h_n，满足

$$h_n(e) = n; \tag{13}$$

以及对任意的$m \in N$有

$$h_n(m^{+}) = h_n(m) + n. \tag{14}$$

证 **唯一性** 若还存在这样一个映射k_n，则当$m = e$时，显有$h_n(e) = k_n(e) = n$。假设对某个m有$h_n(m) = k_n(m)$，那么，由式(14)得

$$k_n(m^{+}) = k_n(m) + n = h_n(m) + n = h_n(m^{+}).$$

因此，由归纳证明原理就推出对一切$m \in N$有$h_n(m) = k_n(m)$。这就证明了唯一性。

存在性 当$n = e$时，取

$$h_e(m) = m, \qquad m \in N. \tag{15}$$

显见条件(13)成立。由式(1)知，$h_e(m^{+}) = m^{+} = m + e = h_e(m) + e$。所以条件(14)也成立。所以当$n = e$时，映射存在，假设对$n$存在这样的映射$h_n(m)$。对$n^{+}$我们取

$$h_{n^{+}}(m) = h_n(m) + m. \tag{16}$$

这样，当$m = e$时，由式(16)，(13)及式(1)推出：

$$h_{n^{+}}(e) = h_n(e) + e = n + e = n^{+}.$$

所以条件(13)成立。利用式(16)，(14)，交换律，结合律及式(1)就得

$$h_{n^{+}}(m^{+}) = h_n(m^{+}) + m^{+} = (h_n(m) + n) + (m + e)$$

$$= (h_n(m) + m) + (n + e) = h_{n^+}(m) + n^+,$$

这就证明了对 h_{n^+} 条件（14）也成立。由归纳证明原理就证明了引理的结论。

定理 3 的证明 *存在性* 对任一 $n \in \boldsymbol{N}$，设 h_n 是引理 4 中确定的映射．现定义二元运算 π 为：

$$n\pi m = h_n(m), \quad n \in \boldsymbol{N}, \ m \in \boldsymbol{N}. \tag{17}$$

我们来证明这个二元运算满足条件(11)和(12)。由式(13)得

$$n\pi e = h_n(e) = n,$$

所以条件(11)成立。由式(14)得

$$n\pi m^+ = h_n(m^+) = h_n(m) + n = (n\pi m) + n,$$

即条件(12)成立。这就证明了存在性。

唯一性 设二元运算 τ 也满足条件(11)和(12)。当 $m = e$ 时，对任意的 $n \in \boldsymbol{N}$，由式(11)得：

$$n\pi e = n = n\tau e.$$

假设对某个 m 使对任意的 $n \in \boldsymbol{N}$ 有

$$n\pi m = n\tau m.$$

那么，对 m^+ 及任意的 $n \in \boldsymbol{N}$，由式(12)及上式就推出：

$$n\pi m^+ = (n\pi m) + n = (n\tau m) + n = n\tau m^+.$$

所以，由归纳证明原理推出：对任意的 $n \in \boldsymbol{N}$，$m \in \boldsymbol{N}$ 有 $n\pi m = n\tau m$ 成立，这就证明了唯一性。

基于定理 3 就可以定义乘法。

乘法 我们把满足定理 3 的二元运算 π 称为是自然数集合 $\boldsymbol{N}$ 上的乘法运算（或乘法），并记作

$$n\pi m = n \cdot m, \quad n, m \in \boldsymbol{N}.$$

下面来证明乘法运算所满足的规律及性质．

（6）**乘法右分配律** 对任意的 $a, b, c \in \boldsymbol{N}$ 有

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c). \tag{18}$$

证 对 c 用归纳证明原理证明。当 $c = e$ 时，由乘法定义得

$$(a + b) \cdot e = a + b = (a \cdot e) + (b \cdot e),$$

所以结论成立。假设当 $c=n$ 时结论成立。那么，当 $c=n^+$时，由乘法定义、假设、及加法的交换律与结合律可得

$$\begin{aligned}(a+b)\cdot n^+ &= ((a+b)\cdot n)+(a+b)\\ &= ((a\cdot n)+(b\cdot n))+(a+b)\\ &= ((a\cdot n)+a)+((b\cdot n)+b)\\ &= (a\cdot n^+)+(b\cdot n^+),\end{aligned}$$

所以结论对 $c=n^+$ 也成立。证毕。

(7) 对任意的 $a\in\boldsymbol{N}$ 有

$$e\cdot a=a. \tag{19}$$

证 对 a 用归纳证明原理证明。当 $a=e$ 时由乘法定义知(19)成立。假设当 $a=n$ 时结论成立。当 $a=n^+$时，由乘法定义、假设、及加法定义（即式(1))得

$$e\cdot n^+=(e\cdot n)+e=n+e=n^+,$$

所以结论也成立。证毕。

(8) **乘法交换律** 对任意的 $a,b\in\boldsymbol{N}$ 有

$$a\cdot b=b\cdot a. \tag{20}$$

证 对 b 用归纳证明原理证明。当 $b=e$ 时，由乘法定义知，式（20）就是式(19)，所以结论成立。假设当 $b=n$ 时结论成立。当 $b=n^+$时，由加法定义、性质(6)、假设、性质(7) 及乘法定义得到

$$\begin{aligned}n^+\cdot a &= (n+e)\cdot a=(n\cdot a)+(e\cdot a)\\ &= (a\cdot n)+a=a\cdot n^+,\end{aligned}$$

所以结论也成立。证毕。

(9) **乘法结合律** 对任意的 $a,b,c\in\boldsymbol{N}$ 有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c). \tag{21}$$

证 对 c 用归纳证明原理证明。当 $c=e$ 时，由乘法定义得 $(a\cdot b)\cdot e=a\cdot b=a\cdot(b\cdot e)$，所以结论成立。假设当 $c=n$ 时结论成立。那么，当 $c=n^+$时，由乘法定义、假设、性质(8)及性质(6)得到

$$
\begin{aligned}
(a\cdot b)\cdot n^{+} &= ((a\cdot b)\cdot n)+(a\cdot b)\\
&= (a\cdot(b\cdot n))+(a\cdot b)\\
&= ((b\cdot n)\cdot a)+(b\cdot a)\\
&= ((b\cdot n)+b)\cdot a\\
&= (b\cdot n^{+})\cdot a\\
&= a\cdot(b\cdot n^{+}),
\end{aligned}
$$

所以结论也成立。证毕。

(10) **乘法右相消律** 对任意的 $a,b,c\in \boldsymbol{N}$，从 $a\cdot c=b\cdot c$ 成立可推出 $a=b$。

证 用反证法，若 $a\neq b$，由加法性质（5）知，必有 $a=b+x$ 或 $b=a+y$ 成立。不妨设 $a=b+x$ 成立，由条件及乘法性质（6）知

$$b\cdot c=a\cdot c=(b+x)\cdot c=(b\cdot c)+(x\cdot c),$$

而由加法性质（4）知这是不可能的，矛盾。证毕。

由乘法交换律知，乘法的左分配律及左相消律均成立。请读者自己写出。

§3 顺序(大小)关系

基于§2中的加法性质（5），我们可以在自然数集合 $\boldsymbol{N}$ 中引进顺序（即大小）的概念。

顺序（即大小） 对给定的 $a,b\in \boldsymbol{N}$，如果存在 $x\in \boldsymbol{N}$，使得 $b=a+x$，那么，我们就说 b 在 a 之后（或 a 在 b 之前），也说 b 大于 a（或 a 小于 b），记作

$$b>a \quad 或 \quad a<b.$$

由定义及§2中的加法性质（5）立即推出

定理1 对任意的 $a,b\in \boldsymbol{N}$，

$$a=b,\qquad a>b \quad 或 \quad a<b,$$

有且仅有一式成立。

容易证明有以下性质成立。

(1) 对任意的 $a\in \boldsymbol{N}$ 有 $a^+>a$。

(2) 对任意的 $a\in \boldsymbol{N}$ 有 $a\geqslant e$，即有 $a=e$ 或 $a>e$ 成立。

(3) 由 $a>b$，$b>c$ 可推出 $a>c$。

(4) $a+x>b+x \Longleftrightarrow a>b$。

(5) $a>b \Longleftrightarrow a\geqslant b^+$。

(6) 对任意的 $a\in \boldsymbol{N}$，不存在 m 使得 $a^+>m>a$。

证 由 $a^+=a+e$ 推出 (1)。当 $a\neq e$ 时，由 §1 定理 2 推出 (2)，(3)直接由定义及加法结合律推出。(4) 可这样证：由定义知 $a>b$ 即 $a=b+y$，由此及加法相消律及交换律、结合律知，它等价于 $a+x=(b+x)+y$，而这就是 $a+x>b+x$，下面来证(5)。$a>b$ 就是 $a=b+x$，由(2)知 $x\geqslant e$，由此及(4)推出 $b+x\geqslant b+e=b^+$（用到加法交换律），所以 $a\geqslant b^+$。利用(1)和(3)立即推出，若 $a\geqslant b^+$ 则必有 $a>b$。最后，用反证法来证(6)，假设 m 存在。我们有

$$a+e=a^+=m+x, \qquad m=a+y.$$

进而得 $a+e=(a+y)+x$，由此及加法结合律、相消律得

$$e=y+x,$$

即 $e>x$，这和性质(2)矛盾。所以 m 不存在。

下面来证明自然数集合 $\boldsymbol{N}$ 的两个重要性质。

定理2（最小自然数原理） 自然数集合 $\boldsymbol{N}$ 的任一非空子集 T 必有最小元素存在，即存在自然数 $t_0\in T$，使对任意的 $t\in T$，必有 $t_0\leqslant t$。

证 考虑由所有这样的自然数 s 组成的集合 S：对任意的 $t\in T$ 必有 $s\leqslant t$。由性质(2)知 $e\in S$，所以 S 非空。此外，若 $t_1\in T$（T 非空所以必有 t_1），则 $t_1+e>t_1$，所以 $t_1+e\notin S$。由这两点及归纳公理就推出：必有 $s_0\in S$ 使得 $s_0+e\notin S$（为什么）.我们来证明这一 s_0 必属于 T。因若不然，由集合 S 的定义知，对任意的 $t\in T$ 必有 $t>s_0$ 成立，由此及性质 (5)推出，对任意的 $t\in T$ 必有 $t\geqslant s_0^+=s_0+e$。但这由定义知 $s_0+e\in S$，矛盾。取 $t_0=s_0$ 就证明了定理。

定理3（最大自然数原理） 设M是自然数集合 $\boldsymbol{N}$ 的非空子集，若M有上界，即存在 $a\in \boldsymbol{N}$ 使对任意的 $m\in M$ 有 $m\leqslant a$，那么，必有 $m_0\in M$，使对任意的 $m\in M$ 有 $m\leqslant m_0$，即 m_0 是M中的最大自然数。

证 考虑由所有这样的自然数 t 组成的集合T：对任意的 $m\in M$ 必有 $m\leqslant t$。由条件知 $a\in T$，所以非空。由定理 2 知T中有最小自然数存在，设为 t_0。我们来证明 $t_0\in M$。若不然，对任意的 $m\in M$ 必有 $m<t_0$。由此及(2)知 $t_0\neq e$。因而由§1定理 2 知存在 $t_1\in \boldsymbol{N}$，$t_0=t_1^+$。由(5) 知对任意的 $m\in M$，$m^+\leqslant t_0$，所以，$m^+\leqslant t_1^+$，由此即得 $m\leqslant t_1$（为什么）。这表明 $t_1\in T$，但 $t_1<t_0$这和t_0的最小性矛盾。取 $m_0=t_0$就证明了定理。

至此，我们用公理化方法定义了抽象自然数集合 $\boldsymbol{N}$，并严格地建立了它的全部基本知识，我们所十分熟悉的由§1式(1)给出的自然数就是它的一个具体模型：规定

$$e=1,2=1^+,3=2^+,4=3^+,5=4^+,6=5^+,$$

$$7=6^+,8=7^+,9=8^+,10=9^+,11=10^+,\cdots,$$

并利用十进位记数法的规定依次写出各数。这样，我们所熟悉的关于§1式(1)给出的自然数的加法、乘法、大小、以及各种运算规则和性质，同这里严格建立起来的相应知识是完全一致的。所以，我们就用由满足 Peano 公理的集合 $\boldsymbol{N}$ 来表示由§1式 (1)给出的全体正整数组成的集合。

要说明的一点是，在有的书上把数 0 也算作自然数，也就是说把 Peano 公理中的元素 e 具体规定时定为0．这时，在定义加法运算、乘法运算、与大小关系时都要作相应的改变，以使和我们熟悉的知识相一致①．有兴趣的读者可以自己作这样的讨论，这也是熟悉公理化方法的一个很好的练习。

以上我们建立了自然数即正整数的严格理论。进而，就可引

① 可参看聂灵沼和丁石孙合著的《代数学引论》（高等教育出版社，1989）第零章§2。本附录的内容的进一步讨论也可参看这一章。

进整数集合——由正、负整数及零组成的集合，及有理数集合，并在其中严格地建立起我们所熟知的知识。这些就不讨论了，有兴趣的读者可以自己做这一有益的工作。

在结束本附录时，我们来简单地讨论一下最小自然数原理和归纳公理的关系。在有一些书上说：这两者等价，或由前者可推出后者，并给出了证明。应该说这样的提法是不确切的，证明是不严格的。因为“大小”关系是在 Peano 公理——它包括归纳公理——的基础上引进、并证明关于它的性质的，所以，当我们说：“可由最小自然数原理来推出归纳公理”时，一个逻辑上的问题是：最小自然数原理中的“大小”概念是怎样定义的？如果不加说明，那么这种推导就有在前提中已包含了结论的毛病，因而是有缺陷的；如果给出和归纳公理无关的“大小”关系的定义，那么就立即出现“自然数”究竟是以怎样的公理体系来定义的问题。这里我们不作深入讨论，只证明以下的结论。

定理4 归纳公理和以下的**非后继元素原理**等价：设 S 是 $\boldsymbol{N}$ 的一个非空子集，那么，必有 $s_0\in S$，使得 s_0 不是 S 中的任一元素的后继，以及当 $S=\boldsymbol{N}$ 时，e 是 $\boldsymbol{N}$ 中的唯一具有这样性质的元素。也就是说，在由 Peano 公理定义的自然数集合 $\boldsymbol{N}$ 中，非后继元素原理一定成立；反过来，如果非空集合 $\boldsymbol{N}$ 满足 Peano 公理中的 (i),(ii),(iii) 及(iv)′——非后继元素原理，那么，在这集合 $\boldsymbol{N}$ 中归纳公理成立。

证 先证第一部分。若 $e\in S$，则结论成立；若 $e\notin S$，考虑 $\boldsymbol{N}$ 中所有不属于 S 的元素组成的集合，记作 T。显见，$e\in T$。由于 S 非空，所以 $T\subset\boldsymbol{N}$，即 T 是 $\boldsymbol{N}$ 的真子集。因此，由归纳公理知（为什么）：必有 $n_0\in T$，$n_0^+\notin T$。这样就有 $n_0\notin S$，$n_0^+\in S$。由此及公理 (iii) 知 S 中的任一元素一定不以 n_0^+ 为其后继元素。取 $s_0=n_0^+$就满足要求。再证后一部分，若满足公理 (i),(ii),(iii)及(iv)′的非空集合 $\boldsymbol{N}$ 中归纳公理不成立，即存在 $\boldsymbol{N}$ 的非空子集 S，$e\in S$，以及若 $n\in S$ 必有 $n^+\in S$，但 $S\subset\boldsymbol{N}$，即 S 是 $\boldsymbol{N}$ 的真子

集。设T是N中所有不属于S的元素组成的集合。显见，T非空且$e\notin T$。由公理(iv)′知，必有$t_0\in T$，使得t_0不是T中任一元素的后继。由于$e\notin T$所以$t_0\neq e$。由公理（iv)′的第二部分知必有$n_0\in N$使$n_0^+=t_0$，由此及t_0的性质知$n_0\notin T$，因此$n_0\in S$。但由S满足的条件知必有$n_0^+=t_0\in S$，这和$t_0\in T$矛盾。证毕。

粗略地说，这里的“非后继元素原理”就相当于定义了“大小”关系后的“最小自然数原理”.在定理4的意义下，它们是等价的，以上都是在Peano公理的框架下，即在“后继”这一关系及对它所规定的性质之下，来讨论这些问题的。应该指出的是：“大小”、“顺序”即“序”的概念是集合元素的一种重要的基本的二元关系。在以上讨论中，是从二元关系——“后继”——出发，假定这一关系满足Peano公理（特别是归纳公理（iv)，由定理4知也就是非后继元素公理(iv)′)，先建立加法运算，然后再引进二元关系——“顺序”关系的。进而证明了有关这一关系的两个性质：最小元素原理与最大元素原理(即定理2和定理3)。反过来，可以先引进二元关系——“序”，要求它满足包括最小元素原理、最大元素原理在内的适当的公理体系来刻画自然数集合，这就和用Peano公理来刻画自然数就完全不同了.这些将安排在习题中。这些习题表明，在这种刻画自然数集合的公理体系中提出的最小元素原理要比归纳公理弱。

习　　题

1．在自然数集合N中证明：

(i) 若$a>b$，$c>d$则$a+c>b+d$，$a\cdot c>b\cdot d$；

(ii) 若$a=b\cdot c$，则$a\geqslant b$，等号当且仅当$c=e$时成立；

(iii) $a\cdot b\geqslant a\cdot c\Longleftrightarrow b\geqslant c$。

2．在抽象的自然数集合N以§3式(1)定义后，根据加法和乘法的定义证明：

(i) $1+1=2$，$1+2=3$，$2+2=4$，$2+3=5$，

$2+4=3+3=6$；

(ii) $2\cdot2=4$，$2\cdot3=6$，$3\cdot4=2\cdot6=12$。

3．具体举例说明 Peano 公理的（i），(ii)，(iii)，(iv) 这四条公理中，随便去掉一条后，可以找到一个集合M它满足剩下的三条公理，且M和自然数集合 $\boldsymbol{N}$ 本质上是不同的。

4．设 $P(n)$ 是一和自然数有关的命题，$n_0\in\boldsymbol{N}$。若（i）命题 $P(n_0)$成立；以及（ii）如果对某个 $n\geqslant n_0$，命题 $P(n)$成立，则命题 $P(n^+)$也成立，那么，命题 $P(n)$对所有的 $n\geqslant n_0$都成立。

5．一个集合M称为**有序集**，如果在这集合中定义了一个二元关系，叫作序，记作$\leqslant$，满足以下条件：

（1）自反性。对所有的 $x\in M$ 有 $x\leqslant x$；

（2）反对称性。若 $x\leqslant y$ 且 $y\leqslant x$，则 $x=y$；

（3）传递性。若 $x\leqslant y$ 且 $y\leqslant z$，则 $x\leqslant z$。

此外，在有序集中 $x<y$ 表示 $x\leqslant y$ 且 $x\neq y$；$x\geqslant y$ 就是 $y\leqslant x$；以及 $x>y$ 表示 $x\geqslant y$ 且 $x\neq y$。证明：

(i) 在有序集中，$x=y$，$x<y$，$y<x$ 至多有一个成立；

(ii) 若 $x<y$，$y<z$ 则 $x<z$；

(iii) 设 S 是一个非空集合，T 是由 S 的所有子集组成的集合。证明：如果把集合的包含关系 $A\subseteq B$ 作为序 $A\leqslant B$，那么，T 是一个有序集；

(iv) 在通常的非负整数集合中，如果把整除关系 $a|b$ 作为序 $a\leqslant b$，那么，它是一个有序集。（注意：对有序集M中的任意两个元素 x,y，不一定要有 $x\leqslant y$ 或 $y\leqslant x$ 成立，它们可以没有这种序关系）。

6．有序集称为是**全序集**，如果它的任意两个元素 x,y，序关系 $x\leqslant y$ 或 $y\leqslant x$ 至少有一个成立。这种序也叫作全序。证明：

(i) 第 5 题的（iii）（当S多于一个元素时），及（iv）中的有序集都不是全序集；

(ii) 通常的自然数集合，整数集合，有理数集合，实数集合，

及它们的子集，在把通常的不大于关系 $x\leqslant y$ 作为序 $x\preccurlyeq y$ 时，都是全序集。

7．设M是一个全序集。我们把命题："在M的任一非空子集S中，必有 $s_0\in S$ 使对任意的 $s\in S$ 必有 $s_0\preccurlyeq s$ 成立"称为**最小元素原理**或**良序原理**。这一原理成立的集合称为**良序集**。

(i) 举出这一原理成立和不成立的全序集的具体例子；

(ii) 证明在良序集M中，对任一 $a\in M$，只要 a 不是M的最大元素（即对任意的 $m\in M$ 有 $m\preccurlyeq a$），就必有唯一的 $a^*\in M$，使得 $a\prec a^*$，以及对任意的 $m\in M$，$a\prec m\prec a^*$都不成立。

8．设M是一个全序集，我们把命题："M的任一非空子集S，若有上界，即有 $a\in M$ 使对任意的 $s\in S$ 有 $s\preccurlyeq a$，则必有 $s_0\in S$，使对任意的 $s\in S$ 有 $s\preccurlyeq s_0$"称为**最大元素原理**。

(i) 证明：如果在全序集M中最大元素原理成立，则对任一 $a\in M$，只要 a 不是M的最小元素（即对所有的 $m\in M$ 有 $a\preccurlyeq m$），那么，必有唯一的 $a^0\in M$ 使得 $a^0\prec a$，以及对任意的 $m\in M$，$a^0\prec m\prec a$ 都不成立；

(ii) 举出这一原理成立和不成立的具体例子；

(iii) 举出良序原理和最大元素原理同时成立、同时不成立、或只有一个成立的各种具体例子；

(iv) 证明：从良序原理和(i)中的 a^0 的存在性可推出最大元素原理。

9．设M是一个全序集。在M中(i) 良序原理成立；(ii) 没有最大元素，即不存在 $a\in M$ 使对任意的 $m\in M$有 $m\preccurlyeq a$；

(iii) 最大元素原理成立。那末，如果把M中的每个 a 所对应的a^*(见第 7 题)看作是 a 的后继元素，则在集合M中 Peano 公理全部成立。这就给出了自然数集合的又一公理化定义。

10．第 9 题中的 (iii)可用(iii)′："对任一 $a\in M$，只要 a 不是M的最小元素（见第 8 题)，则必有唯一的 $a^0\in M$使得 $a^0\prec a$，以及对任意的 m，$a^0\prec m\prec a$ 都不成立"。来代替，而结论仍然成立。

附录二 $Z[\sqrt{-5}]$——算术基本定理不成立的例子

设集合

$$\boldsymbol{Z}[\sqrt{-5}]=\{\alpha=a+b\sqrt{-5}:\ a,b\in\boldsymbol{Z}\}.$$

容易验证，在这个集合中，对通常复数的加法、减法及乘法运算是封闭的，但不一定总可以作除法运算，例如，不存在 $\gamma\in\boldsymbol{Z}[\sqrt{-5}]$ 使得 $1+\sqrt{-5}=2\gamma$。但在集合

$$\boldsymbol{Q}(\sqrt{-5})=\{\alpha=r+s\sqrt{-5}:\ r,s\in\boldsymbol{Q}\}$$

中，对通常复数的加、减、乘及除运算都是封闭的。因为当 $\alpha=r+s\sqrt{-5}\neq0$时，

$$\frac{1}{\alpha}=\frac{1}{r+s\sqrt{-5}}=\frac{r-s\sqrt{-5}}{r^2+5s^2}$$

$$=\frac{r}{r^2+5s^2}-\frac{s}{r^2+5s^2}\sqrt{-5}\in\boldsymbol{Q}(\sqrt{-5}).$$

显见，$\boldsymbol{Z}[\sqrt{-5}]\subset\boldsymbol{Q}(\sqrt{-5})$。由上式容易推出：$\alpha,\alpha^{-1}$ 同时属于 $\boldsymbol{Z}[\sqrt{-5}]$的充要条件是 $s=0,r=\pm1$，即 $\alpha=\pm1$。

如同在 $\boldsymbol{Z}$ 中一样，在 $\boldsymbol{Z}[\sqrt{-5}]$中可引进整除、不可约数等概念。

定义1（$\boldsymbol{Z}[\sqrt{-5}]$ 中的整除） 设 $\alpha,\beta\in\boldsymbol{Z}[\sqrt{-5}]$，$\alpha\neq0$。若有 $\gamma\in\boldsymbol{Z}[\sqrt{-5}]$ 使得 $\beta=\alpha\gamma$，那么就说 **β 可被 α 整除**，记作 $\alpha|\beta$，且称 β 是 α 的**倍数**，α 是 β 的**约数（除数、因数）**。β 不能被 α 整除就记作 $\alpha\nmid\beta$。

上面已经证明：1 的约数是 ±1。对任一 $\beta\in\boldsymbol{Z}[\sqrt{-5}]$（$\beta\neq0$），$\pm1,\pm\beta$ 一定是 β 的约数，称为是 β 的显然约数，其它的约数称为是 β 的非显然约数。例如：

$$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5}),\qquad(1)$$

所以，$\pm 3, \pm(2+\sqrt{-5}), \pm(2-\sqrt{-5})$ 都是 9 的非显然约数。

$$29=(3+2\sqrt{-5})(3-2\sqrt{-5}),$$

所以，$\pm(3+2\sqrt{-5}), \pm(3-2\sqrt{-5})$都是29的非显然约数。

定义2（$\boldsymbol{Z}[\sqrt{-5}]$中的不可约数） 设$\xi \in \boldsymbol{Z}[\sqrt{-5}]$，$\xi \neq 0, \pm 1$。如果$\xi$没有非显然约数，则称$\xi$是不可约数；不然就称$\xi$是**合数**。

29是$\boldsymbol{Z}$中的不可约数，但它不是$\boldsymbol{Z}[\sqrt{-5}]$中的不可约数。下面来证明：$3, 2\pm\sqrt{-5}$都是不可约数。用反证法，若 3 不是不可约数，则有

$$3=(a+b\sqrt{-5})(c+d\sqrt{-5}), \quad a,b,c,d \in \boldsymbol{Z},$$

且$a+b\sqrt{-5} \neq \pm 1$，$c+d\sqrt{-5} \neq \pm 1$。易知

$$3=(a-b\sqrt{-5})(c-d\sqrt{-5}).$$

两式相乘得

$$\begin{aligned} 9 &= (a^2+5b^2)(c^2+5d^2) \\ &= a^2c^2+5(b^2c^2+a^2d^2)+25b^2d^2. \end{aligned}$$

所以必有$bd=0$。若$b=0$，则

$$9=a^2c^2+5a^2d^2.$$

所以$a^2 \mid 9$，即$a=\pm 1$或± 3。但$a+b\sqrt{-5} \neq \pm 1$，所以必有$a=\pm 3$，因而得

$$1=c^2+5d^2.$$

即必有$c=\pm 1, d=0$，但这和$c+d\sqrt{-5} \neq \pm 1$矛盾。同样证$d=0$也不可能。所以 3 是不可约数。

若$2+\sqrt{-5}$不是不可约数，则有

$$2+\sqrt{-5}=(a+b\sqrt{-5})(c+d\sqrt{-5}), \quad a,b,c,d \in \boldsymbol{Z},$$

且$a+b\sqrt{-5} \neq \pm 1$，$c+d\sqrt{-5} \neq \pm 1$。易知

$$2-\sqrt{-5}=(a-b\sqrt{-5})(c-d\sqrt{-5}).$$

两式相乘得

$$9=(a^2+5b^2)(c^2+5d^2).$$

同上面推理一样，由此必得$a+b\sqrt{-5}=\pm1$，或$c+d\sqrt{-5}=\pm1$，矛盾。所以$2+\sqrt{-5}$是不可约数，上面已同时证明了$2-\sqrt{-5}$是不可约数（为什么）。

显见，$3\neq\pm(2\pm\sqrt{-5})$。所以式(1)给出了9在$\boldsymbol{Z}[\sqrt{-5}]$中的两个不同的不可约数分解式。这表明在$\boldsymbol{Z}[\sqrt{-5}]$中§6定理2——算术基本定理不成立。

在$\boldsymbol{Z}$中对不可约数有第一章§6定理1成立，但这在$\boldsymbol{Z}[\sqrt{-5}]$中也不成立，即若$\xi$是$\boldsymbol{Z}[\sqrt{-5}]$中的不可约数，$\xi\mid\alpha\beta$，则$\xi\mid\alpha$，或$\xi\mid\beta$不一定必有一个成立。这因为由以上讨论知，

$$3\mid 9=(2+\sqrt{-5})(2-\sqrt{-5}),\quad 3\nmid 2\pm\sqrt{-5},$$

以及

$$2\pm\sqrt{-5}\mid 9=3\cdot3,\quad 2\pm\sqrt{-5}\nmid 3.$$

但我们可以证明下面的结论：

定理1 设$\pi\in\boldsymbol{Z}[\sqrt{-5}]$，$\pi\neq0,\pm1$。若对任意的$\alpha,\beta\in\boldsymbol{Z}[\sqrt{-5}]$，从$\pi\mid\alpha\beta$必可推出$\pi\mid\alpha$或$\pi\mid\beta$至少有一个成立，则$\pi$一定是不可约数。

证 为使推导简单，引进下面记号。对$\sigma=r+s\sqrt{-5}\in\boldsymbol{Q}(\sqrt{-5})$，记$\sigma'=r-s\sqrt{-5}$，及

$$N(\sigma)=\sigma\sigma'=r^2+5s^2. \tag{2}$$

容易验证（留给读者）：

$$N(\sigma_1\sigma_2)=N(\sigma_1)N(\sigma_2),\quad \sigma_1,\sigma_2\in\boldsymbol{Q}(\sqrt{-5}); \tag{3}$$

$$N(\alpha)\in\boldsymbol{N},\quad \alpha\in\boldsymbol{Z}[\sqrt{-5}]; \tag{4}$$

$$N(\alpha)\mid N(\beta),\quad \alpha\mid\beta,\ \alpha,\beta\in\boldsymbol{Z}[\sqrt{-5}], \tag{5}$$

$N(\alpha)\mid N(\beta)$是表示在$\boldsymbol{Z}$中$N(\alpha)$整除$N(\beta)$；以及若$\alpha\in\boldsymbol{Z}[\sqrt{-5}]$，则

$$\alpha = \pm 1 \Longleftrightarrow N(\alpha) = 1. \tag{6}$$

下面用反证法来证明定理。若 π 不是不可约数，则必有 $\alpha \neq \pm 1$, $\pm\pi$，满足 $\alpha|\pi$，即有

$$\pi = \alpha\beta, \quad \alpha, \beta \in \boldsymbol{Z}[\sqrt{-5}], \quad \alpha \neq \pm 1, \pm\pi.$$

显见，$\beta \neq \pm 1, \pm\pi$。所以由式(4)和(6)知

$$N(\alpha) > 1, \quad N(\beta) > 1.$$

因此，由式(3) 得

$$N(\pi) > N(\alpha) > 1, \quad N(\pi) > N(\beta) > 1. \tag{7}$$

但由定理条件知 $\pi|\alpha$ 或 $\pi|\beta$ 至少有一个成立。若 $\pi|\alpha$ 则 $N(\pi)|N(\alpha)$，因而有 $N(\pi) \leqslant N(\alpha)$；若 $\pi|\beta$ 则可推出 $N(\pi) \leqslant N(\beta)$，这都和式(7)矛盾。证毕。

那末，在 $\boldsymbol{Z}[\sqrt{-5}]$中有没有满足定理 1 中的性质的 π 存在呢？回答是肯定的。例如$\sqrt{-5}$ 就有这样的性质。设

$$\alpha = a + b\sqrt{-5}, \quad \beta = c + d\sqrt{-5}, \quad a, b, c, d \in \boldsymbol{Z}.$$

若$\sqrt{-5}\,|\,\alpha\beta$，则

$$5 = N(\sqrt{-5})\,|\,N(\alpha)N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2).$$

由第一章 §6定理 1 知，在 $\boldsymbol{Z}$ 中 $5|a^2 + 5b^2$ 或 $5|c^2 + 5d^2$，必有一成立。若 $5|a^2 + 5b^2$，则 $5|a^2$，因而 $5|a$。设 $a = 5a_1$，就有

$$\alpha = 5a_1 + b\sqrt{-5} = \sqrt{-5}\,(b - a_1\sqrt{-5}),$$

即$\sqrt{-5}\,|\,\alpha$。同样，由 $5|c^2 + 5d^2$ 可推出 $\sqrt{-5}\,|\,\beta$。具有这种性质的数比不可约数的要求更强。我们可以引进一个新的概念。

定义3（$\boldsymbol{Z}[\sqrt{-5}]$**中的素数**） 设 $\pi \in \boldsymbol{Z}[\sqrt{-5}]$，$\pi \neq 0, \pm 1$。若对任意的 $\alpha, \beta \in \boldsymbol{Z}[\sqrt{-5}]$，由 $\pi|\alpha\beta$ 可推出 $\pi|\alpha$ 或 $\pi|\beta$ 至少有一个成立，则称 π 是素数。

这样，在 $\boldsymbol{Z}[\sqrt{-5}]$中素数一定是不可约数，但不可约数不一

定是素数。

在 Z 中我们也可以把由第一章§2定义 2 所定义的数称为不可约数，而像定义 3 那样来定义 Z 中的素数（把定义 3 中的 $Z[\sqrt{-5}]$ 都改为 Z 即可）。但由第一章§6定理 1 知，在 Z 中，素数就是不可约数。因此，在 Z 中我们用不到引进两个概念。

应该指出："不可约数"，"素数"的概念是和所讨论的"整数"集合(例如：这里的 Z，$Z[\sqrt{-5}]$)有关的。29 是 Z 中的素数，但不是 $Z[\sqrt{-5}]$中的不可约数；3 是 Z 中的素数，也是 $Z[\sqrt{-5}]$ 中的不可约数，但不是 $Z[\sqrt{-5}]$中的素数；11是 Z 中的素数，也是 $Z[\sqrt{-5}]$ 中的素数。前几个结果前面已证，下面来证最后一个结论。设

$$\alpha = a + b\sqrt{-5}, \qquad \beta = c + d\sqrt{-5}, \qquad a,b,c,d \in Z.$$

若 $11 \mid \alpha\beta$，则

$$121 = N(11) \mid N(\alpha\beta) = N(\alpha)N(\beta) = (a^2+5b^2)(c^2+5d^2).$$

所以在 Z 中 $11 \mid a^2+5b^2$ 或 $11 \mid c^2+5d^2$ 至少有一个成立。若 $11 \mid a^2+5b^2$，由第一章§4例 8 知，必有 $11 \mid a, 11 \mid b$，因而 $11 \mid \alpha$。同理，若 $11 \mid c^2+5d^2$，则 $11 \mid \beta$。因此，11 是 $Z[\sqrt{-5}]$中的素数。

上面讨论表明：虽然表面上"整数"集合 $Z[\sqrt{-5}]$ 和整数集合 Z 很相像，但它们的整除性质是本质上不同的。进一步分析可以看出，我们很难在 $Z[\sqrt{-5}]$中引进"最大公约数"的概念。例如：9 和 $3(2+\sqrt{-5})$。它们的公约数有

$$\pm 1, \pm 3, \pm(2+\sqrt{-5}).$$

无论是把 3 还是$(2+\sqrt{-5})$ 看作是"最大公约数"，都不可能具有第一章§4 定理 7 所刻画的 Z 中的最大公约数所具有的最本质的性质：即公约数一定是"最大公约数"的约数。这一切导致一门新的学科——代数数论的产生。这里不作进一步讨论了。有兴趣的读者可参看潘承洞和潘承彪合著的《初等代数数论》(山东大学出版社，1992)，或其它代数数论基础的教材。

习　题

1. 设 $\alpha, \beta \in \boldsymbol{Z}$。若在 $\boldsymbol{Z}[\sqrt{-5}]$中有 $\alpha|\beta$，则在 $\boldsymbol{Z}$ 中也一定有 $\alpha|\beta$。

2. 证明：$2, 7, 23, 1+\sqrt{-5}$，$3+\sqrt{-5}$ 都是 $\boldsymbol{Z}[\sqrt{-5}]$ 中中的不可约数，但都不是 $\boldsymbol{Z}[\sqrt{-5}]$中的素数。

3. 证明：13，17 都是 $\boldsymbol{Z}[\sqrt{-5}]$中的素数。

4. 设 $r+s\sqrt{-5} \in \boldsymbol{Q}(\sqrt{-5})$，$N(r+s\sqrt{-5})=1$。试问：$r+s\sqrt{-5}$ 一定属于 $\boldsymbol{Z}[\sqrt{-5}]$吗？

5. 设 $\alpha \in \boldsymbol{Z}[\sqrt{-5}]$，$\alpha \neq 0, \pm 1$。证明：(i) α 一定可表为 $\boldsymbol{Z}[\sqrt{-5}]$中的不可约数的乘积；(ii) 若 α 可分解为$\boldsymbol{Z}[\sqrt{-5}]$中的素数的乘积，那么在不计次序和相差乘一个 ± 1 的意义下这分解式是唯一的，而且它的不可约数分解式一定就是素数分解式。

6. 证明：(i) $3, 2+\sqrt{-5}$ 的公约数只有 ± 1；(ii) 不存在 $\alpha, \beta \in \boldsymbol{Z}[\sqrt{-5}]$使得 $3\alpha+(2+\sqrt{-5})\beta=1$。解释这题的意义。

7. 设集合 $\boldsymbol{Z}[\sqrt{-6}]=\{\alpha=a+b\sqrt{-6};\ a, b \in \boldsymbol{Z}\}$。如同讨论 $\boldsymbol{Z}[\sqrt{-5}]$一样来讨论 $\boldsymbol{Z}[\sqrt{-6}]$，指出在 $\boldsymbol{Z}[\sqrt{-6}]$ 中和 $\boldsymbol{Z}[\sqrt{-5}]$中一样，“算术基本定理”不成立，即一个数的不可约数分解式不一定是唯一的。

附录三　初等数论的几个应用

§1　循环比赛的程序表

有N个篮球队进行循环赛，每个队都要和其它的队进行$N-1$场比赛。这样，至少要进行$N-1$轮比赛才能使得各个球队之间都进行了比赛。现在的问题是：

（A）为了实现循环赛，举行$N-1$轮比赛是否足够，最少要举行多少轮比赛；

（B）如何安排每一轮各队之间的比赛，即排出比赛程序表。

首先，N个队进行循环赛时，比赛的总场数：

$$\begin{aligned} S &= (N-1)+(N-2)+\cdots+2+1 \\ &= N(N-1)/2. \end{aligned} \tag{1}$$

其次，在每一轮比赛中最多安排的比赛场数：

$$l=\begin{cases} N/2, & N\text{是偶数}, \\ (N-1)/2, & N\text{是奇数}. \end{cases} \tag{2}$$

由以上两式立即推出：当N是偶数时至少举行$N-1$轮比赛；当N是奇数时至少举行N轮比赛，这时每轮比赛中必有一队轮空。这种不一致的情形很容易统一。当N是奇数时，我们可假想加进一个第$N+1$个队T，并按$N+1$个队来安排比赛程序，凡是在一轮比赛中安排与队T进行比赛的队就轮空。所以，下面我们总假定参赛的队数N是偶数。

现在，我们用同余理论来安排每轮的比赛，从而证明进行$N-1$轮比赛就足够了。对N个队进行编号：$x=1,2,3,\cdots,N$。在第r轮比赛中，以x_r表示与第x队进行比赛的队的编号。这样，安排比赛程序表就是要确定x_r，$1\leqslant r\leqslant N-1$，我们来证明按

下面方法确定的 x_r 就满足要求：

(a) 当 $x\neq N$ 且

$$x\neq\begin{cases} r/2, & r\text{ 为偶数}, \\ (r+N-1)/2, & r\text{ 为奇数} \end{cases} \tag{3}$$

时，取 x_r 满足

$$\begin{cases} x+x_r\equiv r(\bmod\ N-1), \\ 1\leqslant x_r\leqslant N-1. \end{cases} \tag{4}$$

(b) 当

$$x=\begin{cases} r/2, & r\text{ 为偶数}, \\ (r+N-1)/2, & r\text{ 为奇数}, \end{cases} \tag{5}$$

时，取 $x_r=N$。为此，我们需要证明：(i) 在第 $r(1\leqslant r\leqslant N-1)$ 轮比赛中，按这样的安排，必有 $x_r\neq x$ 且不同的队 $x\neq x'$ 的对手也是不同的，即 $x_r\neq x'_r$；(ii) 每一个确定的队 x，在所有这 $N-1$ 轮比赛中的对手是不同的，即当 $r_1\neq r_2$ 时必有 $x_{r_1}\neq x_{r_2}$。

先来证(i)。当 x,x' 都不等于N且满足式(3)时，x_r,x'_r由式(4)确定。若 $x_r=x'_r$ 则由式(4)推出

$$x\equiv x'(\bmod\ N-1).$$

由此及 $1\leqslant x,x'\leqslant N-1$ 知 $x=x'$，所以不可能。若 $x_r=x$ 则由式(4)知

$$2x=2x_r\equiv r(\bmod\ N-1),$$

由此及N是偶数推出必有式(5)成立，这和式(3)矛盾，所以也不可能。这里附带证明了，这时 x_r 也满足式(3)（以 x_r 代 x）。这就证明了除了 $x=N$ 及式(5)确定的一个队（它显然不等于N）之外，在第 r 轮比赛中其它的 $N-2$ 个队恰好两两分组进行比赛。而由(b)知这两个例外的队恰好是分在一组比赛。这就证明了(i)。

再来证(ii)。先对第N队来证明。若 $N_{r_1}=N_{r_2}$，由(b)知

$$N_r=\begin{cases} r/2, & r\text{ 为偶数}, \\ (r+N-1)/2, & r\text{ 为奇数}. \end{cases}$$

所以，

$$2N_r \equiv r \pmod{N-1}.$$

故由 $N_{r_1}=N_{r_2}$ 推出 $r_1 \equiv r_2 \pmod{N-1}$，即 $r_1=r_2$。这就证明了结论(ii)对第N队成立。当 $1 \leqslant x \leqslant N-1$ 时，若 $x_{r_1}=x_{r_2}=N$，则由已经证明的第N队在不同轮的比赛中对手是不同的，就推出 $r_1=r_2$；若 $x_{r_1}=x_{r_2} \neq N$，由(i)知式(3)对 $r=r_1, r_2$ 均成立，因此式(4)对 $r=r_1, r_2$ 也都成立。所以推出 $r_1 \equiv r_2 \pmod{N-1}$，即 $r_1=r_2$。证毕。

下面的表列出了 $N=8$ 时的比赛程序。

r \ x	1	2	3	4	5	6	7	8
1	7	6	5	8	3	2	1	4
2	8	7	6	5	4	3	2	1
3	2	1	7	6	8	4	3	5
4	3	8	1	7	6	5	4	2
5	4	3	2	1	7	8	5	6
6	5	4	8	2	1	7	6	3
7	6	5	4	3	2	1	8	7

§2　如何计算星期几

看一下日历就能知道今天是星期几。但是，如果要问你中华人民共和国成立的日子——1949年10月1日是星期几，或是2000年1月1日是星期几，大概就不一定能很快说出来了。虽然，日期的星期几是以7为周期（即相隔天数为7的倍数的两个日期的星期几是相同的），但是，通常一年的天数365不是7的倍数，而且按现行公历的规定，当年份是4的倍数的年，除了以下规定的年份外，都是闰年，即一年有366天，且这增加的一天定为2月29日，这些例外的年份是：

$$k\times 100,\quad 4\nmid k,\tag{1}$$

即形如

$$1700,\ 1800,\ 1900,\ 2100,\ 2200,\ 2300,\cdots$$

的年份。这种不规则性给我们确定星期几带来了很大的困难。下面我们要利用同余知识来给出一个方便的计算公式。在给出之前，先作一些分析。由于闰年增加的一天是定在2月29日，所以，由于这一天而引起的与确定通常年份的日期的星期几不同的变化，仅发生在闰年的3月1日起到下一年的2月28日。因此为了便于给出一般公式，我们把3月算作是这一年的第一个月，4月算作这一年的第二个月，…，12月算作第十个月，下年的1月算作这一年的第十一个月，及下年的2月算作这一年的第十二个月。在这样的规定下：1991年9月2日就要写为“1991”年“7”月2日；而1991年1月3日就要写为“1990”年“11”月3日。以后我们写出的日期：

$$D=\text{第“}N\text{”年“}m\text{”月 }d\text{ 日}\tag{2}$$

都是按这规定。对星期几我们也给一个数字作为代表：

$$\begin{aligned}&\text{星期日}=0,\ \text{星期一}=1,\ \text{星期二}=2,\ \text{星期三}=3,\\&\text{星期四}=4,\ \text{星期五}=5,\ \text{星期六}=6.\end{aligned}\tag{3}$$

这些代表星期几的数字我们称之为星期数。我们的目的就是找出一个公式来计算由式(2)给出的日期D的星期数，我们记作W_D。

我们来证明：当日期D由式(2)给出时，

$$\begin{aligned}W_D\equiv &d+[(13m-1)/5]+y\\&+[y/4]+[c/4]-2c\pmod 7,\end{aligned}\tag{4}$$

这里c,y由下式确定：

$$N=100\cdot c+y,\quad 0\leqslant y<100.\tag{5}$$

在证明公式(4)之前，先用它来计算几个日期的星期数，同时检验它的正确性。

例1 今天是1991年9月2日，是星期一。下面用公式(4)来

计算．用规定（式(2)）这一日期应写为：

$$D=\text{第“1991”年“7”月2日}.$$

所以，$c=19$，$y=91$，$m=7$，$d=2$。由式(4)得

$$\begin{aligned}W_D&\equiv 2+[90/5]+91+[91/4]+[19/4]-38\\&\equiv 2+18+91+22+4-38\equiv 1(\text{mod }7),\end{aligned}$$

即由公式也算出是星期一。

例2　1949年10月1日是星期几？

这时

$$D=\text{第“1949”年“8”月1日},$$

所以，$c=19$，$y=49$，$m=8$，$d=1$。由式(4)得

$$\begin{aligned}W_D&\equiv 1+[103/5]+49+[49/4]+[19/4]-38\\&\equiv 1+20+49+12+4-38\equiv 6(\text{mod }7).\end{aligned}$$

因此，这天是星期六。

例3　2000年1月1日是星期几？

这时按规定

$$D=\text{第“1999”年“11”月1日}.$$

所以，$c=19$，$y=99$，$m=11$，$d=1$。由式(4)得

$$\begin{aligned}W_D&\equiv 1+[142/5]+99+[99/4]+[19/4]-38\\&\equiv 1+28+99+24+4-38\equiv 6(\text{mod }7).\end{aligned}$$

因此，这天是星期六。

公式(4)的证明　证明的途径是这样的：先求出第N年3月1日，即第“N”年的“1”月1日的星期数，然后求第“N”年“m”月1日的星期数，最后求第“N”年“m”月d日的星期数。

(i) 第“N”年“1”月1日的星期数的计算公式。我们以W_N^0表示第“N”年“1”月1日的星期数。设1601年到第N年中有S年不是闰年，T年是闰年，由于非闰年是365天，$365\equiv 1(\text{mod }7)$，闰年是366天，$366\equiv 2(\text{mod }7)$，以及星期数以7为周期，所以

$$W_N^0\equiv W_{1600}^0+S+2T(\text{mod }7).$$

由此及$S+T=N-1600=100c+y-1600$得

$$W_N^0 \equiv W_{1600}^0 + (100c + y - 1600) + T \pmod 7. \qquad (6)$$

这就归结为求闰年数T。注意到1600年是闰年，以及除了式(1)给出的例外以外，年份是4的倍数的年是闰年的规定，易得

$$T = [(100c + y - 1600)/4] - (c - 16) + [(c - 16)/4]. \qquad (7)$$

由式(6)和(7)推出

$$\begin{aligned} W_N^0 &\equiv W_{1600}^0 + (100c + y - 1600) + 25c - 400 + [y/4] \\ &\quad - (c - 16) + [c/4] - 4 \\ &\equiv W_{1600}^0 + 124c + y - 1988 + [y/4] + [c/4] \\ &\equiv W_{1600}^0 - 2c + y + [y/4] + [c/4] \pmod 7. \end{aligned} \qquad (8)$$

1991年3月1日（即"1991"年"1"月1日）是星期五，即

$$W_{1991}^0 = 5.$$

由此及式(8)(注意到$N = 1991$时$c = 19$，$y = 91$）推出：

$$W_{1600}^0 \equiv 5 + 38 - 91 - 22 - 4 \equiv 3 \pmod 7$$

所以$W_{1600}^0 = 3$，即1600年3月1日（即"1600"年"1"月1日）是星期三。因此，式(8)变为

$$W_N^0 \equiv 3 - 2c + y + [y/4] + [c/4] \pmod 7. \qquad (9)$$

这就是我们所要的计算公式。

(ii) 第"N"年"m"月1日的星期数的计算公式，以$W_{N,m}^0$表这天的星期数。显有$W_N^0 = W_{N,1}^0$。由于每月的天数是：

3月 =	"1"月	31天	9月 =	"7"月	30天
4月 =	"2"月	30天	10月 =	"8"月	31天
5月 =	"3"月	31天	11月 =	"9"月	30天
6月 =	"4"月	30天	12月 =	"10"月	31天
7月 =	"5"月	31天	下年1月 =	"11"月	
8月 =	"6"月	31天			

由此及星期数是以7为周期，推出

$W_{N,1}^0 = W_N^0$，　　$W_{N,2}^0 \equiv W_N^0 + 3 \pmod 7$，

$W_{N,3}^0 \equiv W_N^0 + 5 \pmod 7$，　$W_{N,4}^0 \equiv W_N^0 + 8 \pmod 7$，

$$W_{N,5}^0 \equiv W_N^0 + 10 \pmod 7, \quad W_{N,6}^0 \equiv W_N^0 + 13 \pmod 7,$$
$$W_{N,7}^0 \equiv W_N^0 + 16 \pmod 7, \quad W_{N,8}^0 \equiv W_N^0 + 18 \pmod 7,$$
$$W_{N,9}^0 \equiv W_N^0 + 21 \pmod 7, \quad W_{N,10}^0 \equiv W_N^0 + 23 \pmod 7,$$
$$W_{N,11}^0 \equiv W_N^0 + 26 \pmod 7, \quad W_{N,12}^0 \equiv W_N^0 + 29 \pmod 7.$$

注意到 $29/11 = 2.6\cdots$。经过试算，我们很幸运地发现，以上十二式可以用以下公式统一表出：

$$W_{N,m}^0 \equiv W_N^0 + [(13m - 11)/5] \pmod 7. \tag{10}$$

由此及式(9) 得到

$$W_{N,m}^0 \equiv 1 - 2c + y + [y/4] + [c/4] + [(13m - 1)/5] \pmod 7. \tag{11}$$

这就是我们所要的公式。

当日期 D 由式(2) 给出时，显然有

$$W_D \equiv W_{N,m}^0 + (d - 1) \pmod 7,$$

由此及式(11)就推出公式(4)。证毕。

最后，必须指出的是：以上所说的公历规则是教皇格里哥利十三实行的，是改革了原有的恺撒历，为了使得季节和日历之间的关系协调一致。格里哥利十三于原来恺撒历的1582年10月 5 日(星期五)，把这一天改为1582年10月15日(星期五)，并自此以后按他规定的办法来确定闰年，这就是我们前面所说的。因此，我们的公式只能计算1582年10月15日以后的日期是星期几。还要指出的是，英国和它的殖民地直到1752年才实行格里哥利的历法，把原来恺撒历的1752年 9 月 3 日改为格里哥利历的 1752 年 9 月 14 日。所以，对那些地区公式(4)只适用于计算 1752 年 9 月14日以后日期的星期几。当然，如果以后历法改变，那么我们的公式也要作相应的改变。

§3　电话电缆的铺设

我们知道两条电话线如果长距离的靠近在一起，就会发生干

扰和串音，影响通话质量。铺设多路电话线都是用一段段的环状电缆联结起来实现的。为了保证通话质量，我们希望在一段电缆中相邻的两条电话线，在以后尽可能的若干段电缆中都不相邻。这就需要设计一种连接各段电缆的方法，为了施工方便这种方法又要求是简单而有规律的。

利用同余理论可以证明下面的简单方法可以达到我们的要求。设每段电缆有 m 条电线并以同样顺序编号：$j=1,2,\cdots,m$(见图 1，$m=11$，$j=1,2,\cdots,11$)。我们的连接方法是：选定一个正整数 $s>1$，$(s,m)=1$。把第 l 段电缆中在位置 j 的电线与第 $l+1$ 段电缆中在位置

$$S(j)\equiv 1+(j-1)s(\bmod m),\quad 1\leqslant j\leqslant m, \tag{1}$$

的电线相连接（见图 1，$m=11$，$s=2$)。这种连接方法有以下两个性质：

(a) 若 $j_1\neq j_2$，则 $S(j_1)\neq S(j_2)$。若不然，由 $S(j_1)=S(j_2)$ 及式(1) 推出

$$1+(j_1-1)s\equiv 1+(j_2-1)s(\bmod m).$$

即 $j_1s\equiv j_2s(\bmod m)$。由 $(s,m)=1$ 及 $1\leqslant j_1$、$j_2\leqslant m$ 就得到 $j_1=j_2$。证毕。

(b) 在第 l 段电缆位置 j 上的电线到了第 $l+n$ 段电缆，其位置 $S^{(n)}(j)$满足

$$S^{(n)}(j)\equiv 1+(j-1)s^n(\bmod m),\quad 1\leqslant j\leqslant m. \tag{2}$$

显然有 $S^{(1)}(j)=S(j)$，所以式(2)对$n=1$成立。假设式(2)对$n=k$ $(k\geqslant 1)$ 成立。当 $n=k+1$ 时，由式(1)及假设知

$$S^{(k+1)}(j)=S(S^{(k)}(j))\equiv 1+(S^{(k)}(j)-1)s$$
$$\equiv 1+(j-1)s^{k+1}(\bmod m),$$

即式(2)对 $n=k+1$ 也成立。证毕。

为了尽可能好地保证通话质量，我们希望在第 l 段中的相邻的两条电线 $j,j+1$，能在以后尽可能多的各段中都不相邻，即

$$S^{(n)}(j+1)-S^{(n)}(j)\not\equiv \pm 1(\bmod m) \tag{3}$$

对 $n=1,2,\cdots,n_0-1$ 都成立，而对 $n=n_0$ 不成立（当然对所有的 n，式(3)都成立就更好，但我们的方法不可能），要求 n_0 尽可能地大。这就要求选取适当的 s，若

$$S^{(n_0)}(j+1)-S^{(n_0)}(j)\equiv 1 \text{ 或 } -1 \pmod{m}, \tag{4}$$

则由式(2) 知，它等价于

$$s^{n_0}\equiv 1 \text{ 或 } -1 \pmod{m}. \tag{5}$$

这样，我们的问题就转化为寻找与 m 既约的 s，使得为使式(5)成立的最小正整数 $n_0=n_0(s)$ 是最大的。把这种最大的 n_0 记作 $\lambda_0(m)$。当 m 的素因数分解式为

$$m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$$

时，必有

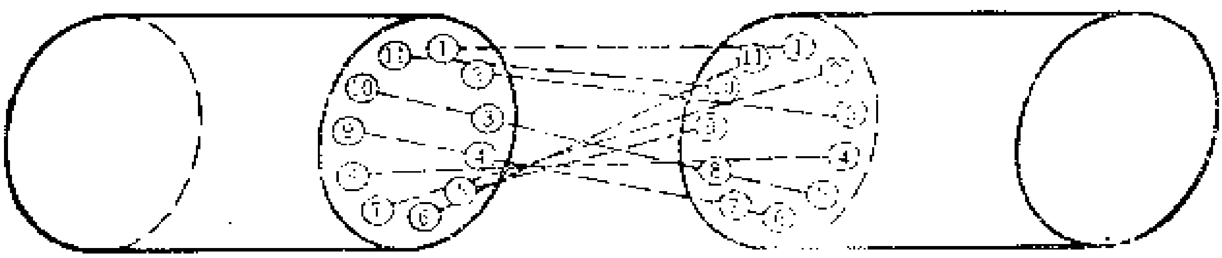
$$s^{\lambda(m)}\equiv 1 \pmod{m}, \quad (s,m)=1,$$

这里 $\lambda(m)$ 由第五章 §1式 7 给出，即

$$\lambda(m)=[2^{c_0},\phi(p_1^{\alpha_1}),\cdots,\phi(p_r^{\alpha_r})], \tag{6}$$

$c_0=0$，当 $\alpha_0=0,1$；$c_0=1$，当 $\alpha_0=2$；$c_0=\alpha_0-2$，当 $\alpha_0\geqslant 3$。所以必有

$$\lambda_0(m)\leqslant\lambda(m)^{①}. \tag{7}$$



j	1	2	3	4	5	6	7	8	9	10	11
$S(j)$	1	3	5	7	9	11	2	4	6	8	10

图 3　电缆连接图（$m=11$，$s=2$）

① 可以证明，必有 $\lambda_0(m)=\lambda(m)$ 或 $\lambda(m)/2$。留给读者。

如何寻求 $\lambda_0(m)$ 和确定相应的 s，可利用指数、原根、指标、指标组的理论来讨论，这里就不讲了。

在图 1 的实例中，$m=11$，容易证明 $\lambda_0(11)=\lambda(11)/2=5$，而 $s=2$ 的确满足所说的要求（证明留给读者）。

通常把确定铺设方法的公式(1)中的 s 称为铺设的离散指数，当 $n_0(s)=\lambda_0(m)$ 时，相应的 s 称为模 m 的最佳离散指数。2就是模11的最佳离散指数。

§4 筹码游戏

筹码游戏是我国古代的一种游戏，在国外称为 Nim 游戏。这种由两个人玩的游戏是这样的：设有 $k(\geq 2)$ 堆筹码，各堆筹码数为

$$n_1, n_2, \cdots, n_k. \tag{1}$$

游戏规则是：两人轮流从这些堆中取筹码，要求

(i) 每次只能从一个堆中取筹码，不能在两个或两个以上的堆中同时取筹码；

(ii) 每次至少取一根筹码，多取不限，直至可把一堆中的筹码完全取走。

最后把筹码取完的人是胜者。显然，这种两人游戏的过程可用 k 元数组 $\{n_1, n_2, \cdots, n_k\}$ 来描述。一人取一次筹码就相当于通过只能把其中某一个分量 n_j 改变为 $n_j'(0\leq n_j'<n_j)$ 的办法，把原来的 k 元数组变为一个新的 k 元数组。这种类型的变换我们称之为 k 元数组的 T 变换。例如：

$$\{5,8,13,7,6,2\}\longrightarrow\{5,8,4,7,6,2\}$$

就是 6 元数组的 T 变换，这里仅把第 3 个分量13变为 4 。

现在，放好了由式(1) 给出的 k 堆筹码，即给定了 k 元数组 $\{n_1, n_2, \cdots, n_k\}$，由 A、B 两人参加，假设由 A 先取。这样，想取胜的 A 所面临的问题是：能不能取一次筹码，即对数组作一次 T 变

换 π_1，使得不管接着 B 怎样取筹码，即作 T 变换，A 总有相应的取法来对付，直至最后保证 A 获胜。这里会面临三种情形：(a)存在这样的 T 变换 π_1，即对放好的这 k 堆筹码，必有方法保证先取者获胜；(b) 不存在这样的 T 变换 π_1，相反的对放好的这 k 堆筹码，必有方法保证后取者获胜；(c) 无法事先肯定是先取者获胜，还是后取者获胜。下面将看到情形(c)是不会出现的(这是一个一般性定理的特例)。

如果我们能够找到 k 元数组的这样一种性质 P：它在 T 变换具有以下的性质：(Ⅰ)具有性质 P 的 k 元数组在作一次 T 变换后，所得的新的 k 元素组一定不具有性质 P；(Ⅱ) 不具有性质 P 的 k 元数组，一定可找到某个 T 变换，使其变为具有性质 P 的 k 元数组；(Ⅲ) k 元数组 $\{0,0,\cdots,0\}$ 具有性质 P，那么，当原始的 k 元数组（即一开始放好的 k 堆筹码）不具有性质 P 时，先取者 A 必有方法取胜；当原始的 k 元数组具有性质 P 时，后取者 B 必有方法取胜。这是因为在第一种情形，先取者 A 必有方法使他取过筹码后所得的 k 元数组具有性质 P，在第二种情形，后取者 B 必有方法使他取过筹码后所得的 k 元数组具有性质 P。由于每取一次筹码总数一定减少及 $\{0,0,\cdots,0\}$ 具有性质 P，所以结论成立。这样，问题就变为寻找这样的性质 P。

当 $k=2$ 时很简单，二元数组 $\{n_1,n_2\}$ 当 $n_1=n_2$ 时称为具有性质 P。显见，它具有前面所说的性质(Ⅰ)，(Ⅱ)，(Ⅲ)。这样，当两堆筹码数不相同，即不具有性质 P 时先取者只要保持每次取筹码后所留下的二元数组具有性质 P ——即 $n_1=n_2$，一定获胜；当两堆筹码数相等，即具有性质 P 时，不管先取者如何取法，留下的二元数组 $\{n_1',n_2'\}$ 一定不具有性质 P，即必有 $n_1'\neq n_2'$，所以，后取者 B 必有方法获胜。

当 $k\geqslant 3$ 时，就很不容易找出这种性质 P 了。这需要利用整数的二进位表示来刻划这种性质，把 k 元数组 $\{n_1,n_2,\cdots,n_k\}$ 中的每个数用二进位数来表示，n_j 写在第 j 行，且对齐二进位的位数，

然后把每列上的数字相加，其和用十进制表示写在第 $k+1$ 行，记为 $\{m_1, m_2, \cdots, m_l\}$。如果这些和 m_t 均为偶数，我们就说这个 k 元数组具有性质 P。例如：对 $\{3,5,8\}$ 有

n_1	3	0	0	1	1
n_2	5	0	1	0	1
n_3	8	1	0	0	0
		1	1	1	2,
		m_1	m_2	m_3	m_4

所以，$\{3,5,8\}$ 不具有性质 P。对 $\{3,5,6\}$ 有

3	0	0	1	1
5	0	1	0	1
6	0	1	1	0
	0	2	2	2,

所以，$\{3,5,6\}$ 具有性质 P。再比如，对 $\{25,43,65\}$ 有

25	0	0	1	1	0	0	1
43	0	1	0	1	0	1	1
65	1	0	0	0	0	0	1
	1	1	1	2	0	1	3,

它不具有性质 P。对 $\{25,43,50\}$ 有

25	0	0	1	1	0	0	1
43	0	1	0	1	0	1	1
50	0	1	1	0	0	1	0
	0	2	2	2	0	2	2,

所以，它具有性质 P。

现在，我们要来证明对 k 元数组这样定义的性质 P 满足条件（Ⅰ），（Ⅱ）和（Ⅲ）。条件（Ⅲ）显然满足。先来证满足条件（Ⅰ）。若 k 元数组 $\{n_1, n_2, \cdots, n_k\}$ 具有性质 P，则对应的 l 元数组 $\{m_1, m_2, \cdots, m_l\}$ 中的每个 m_t 都是偶数。对这数组任作一个 T 变换 π，不妨设是把某一个 n_{j_0} 变为 n'_{j_0}，$0 \leqslant n'_{j_0} < n_{j_0}$，而其它的 $n_j\ (j \neq j_0)$ 不变。这样新的数组为 $\{n_1, \cdots, n_{j_0-1}, n'_{j_0}, n_{j_0+1}, \cdots, n_k\}$，设其相应的 l 元数组是 $\{m'_1, \cdots, m'_l\}$。由于 $n'_{j_0} \neq n_{j_0}$，所以，n'_{j_0} 的二进位表示一定和 n_{j_0} 的不同。设

$$n_{j_0}=a_1a_2\cdots a_t\cdots a_l,\quad a_t=0,1,$$

$$n'_{j_0}=a'_1a'_2\cdots a'_t\cdots a'_l,\quad a'_t=0,1,$$

是它们的二进位表示。那末至少有一个 t_0，使

$$a_{t_0}\neq a'_{t_0}.$$

这仅可能是

$$a_{t_0}=1,a'_{t_0}=0 \text{ 或 } a_{t_0}=0,a'_{t_0}=1.$$

无论哪种情形都使 m_{t_0} 和 m'_{t_0} 的奇偶性不同，具体的说，相应地必有

$$m_{t_0}=m'_{t_0}+1 \text{ 或 } m_{t_0}=m'_{t_0}-1.$$

即 m'_{t_0} 为奇，所以新得到的数组不具有性质 P。这就证明了满足条件(Ⅰ)。

下面来证满足条件(Ⅱ)。设数组$\{n_1,n_2,\cdots,n_k\}$不具有性质P，即相应的 l 元数组$\{m_1,\cdots,m_l\}$中必有一些 m_t 为奇。设 t_0 是最小正整数，使 m_{t_0}为奇。即当 $1\leqslant t<t_0$ 时 m_t 均为偶。显然有$m_{t_0}\geqslant 1$。因而必有一个 n_{j_0}，其二进位表示为：

$$\begin{cases}n_{j_0}=a_1\cdots a_{t_0}a_{t_0+1}\cdots a_l, & a_t=0,1.\\ a_{t_0}=1.\end{cases}$$

假设 $m_1,\cdots,m_l$ 中所有为奇数的是

$$m_{t_0},m_{t_1},\cdots,m_{t_h},\quad 1\leqslant t_0<t_1<\cdots<t_h\leqslant l.$$

构造一个数 n'_{j_0}，它的二进位表示

$$n'_{j_0}=a'_1\cdots a'_t\cdots a'_l$$

这样来规定：

$$\begin{cases}a'_t=a_t, & t\neq t_i,0\leqslant i\leqslant h,\\ a'_t=1-a_t, & t=t_i,0\leqslant i\leqslant h.\end{cases}\tag{2}$$

由于 $a_{t_0}=1$，所以，必有 $0\leqslant n'_{j_0}<n_{j_0}$。对所给的数组作$T$变换

$n_{j_0}\to n'_{j_0}$，其它 n_j 不变，就得到新的 k 元数组$\{n_1,\cdots,n_{j_0-1},n'_{j_0},n_{j_0+1},\cdots,n_k\}$。设它的相应的 l 元数组是$\{m'_1,\cdots,m'_l\}$。由式(2)知

$$m'_t=m_t,\quad t\neq t_i,0\leqslant i\leqslant h,$$
$$m'_t=m_t+1-2a_t,\quad t=t_i,0\leqslant i\leqslant h.$$

因此，所有的 m'_t 均为偶数，即作 T 变换后得的新的 k 元数组具有性质 P。这就证明了条件(Ⅱ)满足。证毕。

前面的$\{3,5,8\}\to\{3,5,6\}$及$\{25,43,65\}\to\{25,43,50\}$都是条件(Ⅱ)满足的例子。

以上仅举了四个简单例子，说明初等数论有广泛而有趣的应用。应该指出最重要的应用是在密码学、信息论、及数值分析等领域，这些应用在很多书中都可找到，并有专门论著，在短短的篇幅中不可能介绍清楚（有的已超出初等数论范围），这里就不讨论了。

习　　题

1．分别排出有 6 个，7 个，9 个，10个运动员参加的循环比赛程序表。

2．证明：在第2轮比赛中第1，2，…，N 队分别和第 N，$N-1$，…，1 队进行比赛。

3．在第 r 轮比赛中，哪个队和第 r 队比赛。

4．芦沟桥事变1937年 7 月 7 日是星期几？

5．第二次世界大战日本宣布无条件投降的1945年 8 月 14 日是星期几？

6．你和你的爸爸、妈妈的生日是星期几？

7．设 $m=16,17,19,22,25,32,36,60,99,100$。

(i) 求 $\lambda_0(m)$；　　(ii) 求 s 使 $\lambda_0(m)=\eta_0(s)$。

8．找出三个 m 使 $\lambda_0(m)=\lambda(m)$。

9. 判定以下数组是否具有性质 P：

$\{2,4,5\}$, $\{3,7,8\}$, $\{6,10,12\}$, $\{16,39,47\}$, $\{29,63,66\}$, $\{7,12,21,25\}$, $\{58,19,23\}$, $\{14,31,33,29,63,66\}$.

附录四　国际数学奥林匹克竞赛中的数论题

国际数学奥林匹克竞赛①，从1959年起到1991年，已经举行了三十二届比赛．大致统计，在总共194道题目中，可以主要用初等数论知识来解的有51题，约占 26.3%．如果加上需要用到一点数论知识去解的题，那所占的比重就更大了．除了第三、五、七、十五届竞赛中没有数论题外，其它各届均有，而且显示出初等数论知识在国际数学奥林匹克竞赛中起着愈来愈重要的作用．除了个别的题外，这些题都是很好的．从根本上说，解这些题只要用第一章所讲的整除理论，但需要高度灵活地直接运用整除理论中的最基本的概念、性质、方法和技巧，是十分不容易做出来的．特别是，一些看来像不定方程的题，千万不要用初等数论中的一般方法去解，因为这样往往适得其反．利用一些同余式、同余类、剩余系的符号、概念与基本性质，对解题是有好处，但决不需要同余和同余方程的进一步的知识．下面列出了这 51 道题，[$x.y$] 表示第 x 届第 y 题．虽然有各种版本的题解，我们希望有兴趣的读者自己去解这些题，我们这里也不给任何提示．

[1.1]　对任意自然数n，分数

$$(21n+4)/(14n+3)$$

都不可约．

[2.1]　求出所有这样的三位数：它被11整除，且所得的商是原三位数的各位数字的平方和．

[4.1]　求具有如下性质的最小自然数：用十进制表示时，它的个位数字是 6．将这个位数字移到最高位数字之前，其它各位

① 关于它的介绍可参看单墫的《数学竞赛史话》，广西教育出版社，1990．

数字保持不动，则所得的数是原数的四倍。

[6.1] (i) 试求使 2^n-1 被 7 整除的所有正整数.

(ii) 证明对任意正整数 n，2^n+1 不能被 7 整除。

[8.1] 在一次竞赛中共出了 A，B，C 三道试题。(i) 在所有参赛学生中共有25人每人至少解出了一道题；(ii) 在没有解出 A 题的学生中，解出 B 题的人数是解出 C 题的人数的两倍；(iii) 在解出 A 题的学生中，只解出 A 题的人数比还解出其它题的人数多一个；以及(iv) 在只解出一道题的学生中，有一半人未解出 A 题。问有多少学生只解出了 B 题。

[9.3] 设 k，m，n 是正整数，$m+k+1$ 是素数且大于 $n+1$。记 $C_s=s(s+1)$。证明：乘积

$$(C_{m+1}-C_k)(C_{m+2}-C_k)\cdots(C_{m+n}-C_k)$$

被乘积 $C_1C_2\cdots C_n$ 整除。

[9.6] 一次体育比赛举行了 n 天，共颁发了 m 个奖章。已知：第一天发了 1 个奖章再加上余下的 $m-1$ 个的 1/7；第二天发了 2 个奖章再加上余下的奖章数的 1/7；每天均是这样发奖章，即第 k 天发了 k 个奖章再加上余下的奖章数的 1/7；最后在第 n 天恰好发了 n 个奖章而无剩余。问比赛进行了几天，总共发了多少个奖章？

[10.2] 设正整数 x 的十进制表示的各位数字之积是 $P(x)$。试求满足 $P(x)=x^2-10x-22$ 的所有正整数 x。

[10.6] 以 $[x]$ 表示不大于实数 x 的最大整数。设 n 是正整数，求 $\sum_{k=0}^{\infty}[(n+2^k)/2^{k+1}]$ 的值。

[11.1] 证明：有无穷多个自然数 a，使得 n^4+a 对于任意的自然数 n 均为合数。

[12.2] 设 a，b，n 是给定的自然数，且都大于 1。再设 A_{n-1} 和 A_n 在 a 进位制中可表为：

$$A_{n-1}=x_{n-1}x_{n-2}\cdots x_0,\quad A_n=x_nx_{n-1}\cdots x_0;$$

B_{n-1} 和 B_n 在 b 进位制中可表为：

$$B_{n-1}=x_{n-1}x_{n-2}\cdots x_0,\quad B_n=x_nx_{n-1}\cdots x_0.$$

这里 $x_{n-1}\neq 0, x_n\neq 0$。证明：当 $a>b$ 时有 $A_{n-1}/A_n<B_{n-1}/B_n$。

[12.1] 试求具有下述性质的所有正整数 n：六个数 $n, n+1, n+2, n+3, n+4, n+5$ 可以分为两组，使得一组中的各数的乘积等于另一组中的各数的乘积。

[13.3] 证明：在数列 $2^n-3(n=2,3,4,\cdots)$ 中一定可取出一个无穷子叙列，其中的数两两互素。

[14.3] 设 m, n 是非负整数。证明 $\dfrac{(2m)!(2n)!}{m!n!(m+n)!}$ 是整数，这里约定 $0!=1$。

[16.1] 有 A, B, C 三人作下列游戏：有三张纸牌，每张上各写一个正整数，分别为 p, q, r，且满足 $p<q<r$。先把这三张牌任意地分给每人一张，再按牌上的数字分给每人以相同数的小球，然后把牌收回但分得的小球仍留在各人手中。再继续这一过程（发牌、分球、收牌），至少要进行两次。在这样进行若干次后游戏结束时，A, B, C 三人分别得到了20、10、9个球。此外，还知道 B 在最后一次分得了 r 个球。问谁在第一次得了 q 个球。

[16.3] 证明：对任意的自然数 n，5一定不能整除

$$\sum_{k=0}^{n}\binom{2n+1}{2k+1}\cdot 2^{3k}.$$

[16.4] 将具有黑白相间的 8×8 个格子的棋盘分为 K 个矩形，且保持方格的完整。还要求满足条件：(i) 每个矩形中白格和黑格数目相等；(ii) 设 a_i 是第 i 个矩形中的白格数目，则 $a_1<a_2<\cdots<a_K$。试求满足这种条件的分法的 K 的最大值，并对这个最大值 K 求出所有可能的 $a_1, a_2, \cdots, a_K$。

[16.6] 设 $P(x)$ 是一个整系数多项式，它的次数 $\deg P\geq 1$。如果有 n 个整数 $k_1, \cdots, k_n$ 使得 $P^2(k_1)=\cdots=P^2(k_n)=1$，那么，必有 $n\leq 2+\deg P$。

[17.2] 设 $a_1<a_2<a_3<\cdots$ 是一个无穷正整数列。证明这个数列中必有无穷多个 a_m 可表为 $a_m=x\cdot a_p+y\cdot a_q$，这里 x,y 是适当的正整数，a_p,a_q 是这数列中的某两个数，$p\neq q$。

[17.4] 设 A 是十进制数 4444^{4444} 的各位数字之和，B 是 A 的十进表示中的各位数字之和。求 B 的十进表示中的各位数字之和。

[17.5] 是否可能在半径为 1 的圆周上选定1975个点，使得其中任意两点间的距离都是有理数？

[18.3] 已知一个长方盒子可用单位立方体（即边长为 1）填满。如果改放尽可能多的体积为两个单位的立方体（保持立方体与盒子的边平行），则盒子的容积恰被填满40%。试求所有这种长方盒子的容积（$\sqrt[3]{2}=1.2599\cdots$）。

[18.4] 求其和为1976的正整数之积的最大值。

[18.6] 定义数列 $u_0=2,u_1=5/2,u_{n+1}=u_n(u_{n-1}^2-2)-u_1$，$n=1,2,\cdots$。证明：$[u_n]=2^{(2^n-(-1)^n)/3}$，$n=1,2,\cdots$，这里 $[x]$ 表示不超过实数 x 的最大整数。

[19.3] 设 $n>2$ 是给定的自然数，集合 $V_n=\{kn+1,k=1,2,\cdots\}$。一个数 $m\in V_n$ 称为是 V_n 中的不可约数，如果不存在 $p\in V_n,q\in V_n$ 使得 $m=p\cdot q$。证明：存在 $r\in V_n$，它可用多于一种的方式表为 V_n 中的不可约数的乘积。

[19.5] 设 a,b 是正整数，$a^2+b^2=q(a+b)+r,0\leqslant r<a+b$。求所有的数对 a,b 使得 $q^2+r=1977$。

[20.1] 试求正整数 m,n，使得(i) 1978^n 与 1978^m 的最后三位数字相等；(ii) $m>n\geqslant 1$；(iii) $m+n$ 取最小值。

[20.3] 设 N 是自然数集合，f,g 都是 $N\to N$ 的严格递增函数。已知：并集 $f(N)\cup g(N)=N$，交集 $f(N)\cap g(N)$ 是空集，且对任意的自然数 n 满足 $g(n)=f(f(n))+1$。试求 $f(240)$ 的表示式。

[21.1] 设 p,q 是自然数，满足

$$\frac{p}{q}=1-\frac{1}{2}+\frac{1}{3}-+\cdots-\frac{1}{1318}+\frac{1}{1319}.$$

证明：p 可被1979整除。

[21.6] 设 A 和 E 是一个正八边形的相对的两个顶点，现有一只青蛙从点 A 开始起跳，如果青蛙在任一个不是 E 的顶点上，那么它可以跳向和这顶点相邻的任一顶点上，当它跳到顶点 E 时就停在那里。设 a_n 是恰好跳 n 步到达 E 的不同的途径的个数。证明：$a_{2n-1}=0$，

$$a_{2n}=\frac{1}{\sqrt{2}}\{(2+\sqrt{2})^{n-1}-(2-\sqrt{2})^{n-1}\},\quad n=1,2,\cdots.$$

[22.3] 设 m,n 在1,2,…，1981中取值。试求满足条件 $(n^2-mn-m^2)^2=1$ 的 m^2+n^2 的最大值。

[22.4] (i) 对怎样的正整数 $n>2$，才可能存在 n 个连续正整数，使得其中最大的正整数是其它 $n-1$ 个数的最小公倍数的约数；

(ii) 对怎样的 n 上述的这种 n 个连续正整数是唯一的。

[23.4] 证明：(i) 设 n 是正整数，若 $x^3-3xy^2+y^3=n$ 有一组整数解 x,y，那么，它至少有三组整数解；

(ii) 当 $n=2891$ 时，上述方程无整数解。

[24.3] 设 a,b,c 是给定的正整数，且两两互素。证明：不能由 $bcx+cay+abz$ (x,y,z 是非负整数) 表出的最大整数是

$$2abc-ab-bc-ca.$$

[25.2] 试求正整数 a,b，使得 7 不能整除 $ab(a+b)$，以及 7^7 能整除 $(a+b)^7-a^7-b^7$。

[25.6] 设 a,b,c,d 是正整数，都是奇数，且满足 $a<b<c<d$。证明：如果有正整数 k,m 使得

$$a+d=2^k,\quad b+c=2^m,$$

那么，必有 $a=1$。

[26.2] 设 n,k 是正整数，k 和 n 互素且满足 $0<k<n$。再设

集合 $M=\{1,2,\cdots,n-1\}$。现对集合M中的每个数 i 涂上兰色或白色，要满足以下条件：(i) i 和 $n-i$ 要涂上同一种颜色；(ii) 当 $i\neq k$ 时，i 和 $|k-i|$ 要涂上同一种颜色。证明：所有的数都涂上同一种颜色。

[27.1] 设正整数 $d\neq 2,5,13$。证明：在集合 $\{2,5,13,d\}$中，一定可找到两个不同元素 a,b 使得 $ab-1$ 不是完全平方数。

[28.3] 证明：对任意的正整数 $n\geqslant 3$，一定可以在笛卡儿坐标平面上取到 n 个点，使得每一对点之间的距离为无理数，以及每三点构成一个非退化三角形，其面积是有理数。

[28.6]① 设正整数 $n\geqslant 2$。证明：如果 k^2+k+n 当 $0\leqslant k\leqslant\sqrt{n/3}$ 时都是素数，则 k^2+k+n 当 $0\leqslant k\leqslant n-2$ 时也都是素数。

[29.3] 设 f 是定义在正整数集合$\boldsymbol{N}$上的函数：$f(1)=1$，$f(3)=3$，以及对任意的 $n\in\boldsymbol{N}$满足

$$f(2n)=f(n),$$
$$f(4n+1)=2f(2n+1)-f(n),$$
$$f(4n+3)=3f(2n+1)-2f(n).$$

试求满足 $n\leqslant 1988$ 及 $f(n)=n$ 的正整数 n 的个数。

[29.6] 设 a,b 是正整数，使得 $ab+1$ 整除 a^2+b^2。证明：$(a^2+b^2)/(ab+1)$ 一定是完全平方数。

[30.1] 证明：集合$\{1,2,\cdots,1989\}$可以分为117个互不相交的子集 $A_i(i=1,2,\cdots,117)$，使得(i) 每个 A_i 含有 17 个元素；(ii) 每个 A_i 中的各元素之和相等。

[30.5] 证明：对任意正整数 n，存在 n 个相邻的正整数，使得它们都不是素数的幂。

[31.2] 设正整数 $n\geqslant 3$，E是由同一圆周上的 $2n-1$ 个不同的点组成的集合。将E中的一部分点染成黑色，其余的点不染色。如果至少有一对黑点，以它们为端点的两条弧中有一条的内部(不

① 实际上和本题相同的结论已出现在郑格于的《数论简易教程》(湖南师专，1982)，第130—132页。

包含端点）恰有 E 中的 n 个点，则称这种染色方式是好的。求最小的k，使将 E 中任意 k 个点染黑的染色方式都是好的。

[31.3] 求出所有大于 1 的整数 n，使得$(2^n+1)/n^2$为整数。

[31.5] 给定一个初始整数值 $n_0>1$ 后，两名竞赛者 A，B按以下规则轮流取整数 $n_1, n_2, n_3, \cdots$：在已知 n_{2k} 时，A可以任取一整数 n_{2k+1}，满足 $n_{2k}\leqslant n_{2k+1}\leqslant n_{2k}^2$；在已知$n_{2k+1}$ 时，B 可以任取一整数 n_{2k+2}，使得 n_{2k+1}/n_{2k+2} 是一个素数的正整数幂。若A取到1990则 A 胜，若 B 取到 1 则 B 胜。试问：对怎样的 n_0，(1) A 有必胜策略，(2) B 有必胜策略，(3) 双方均无必胜策略。

[31.6] 证明：存在一个凸的1990边形，同时具有下面的性质：(i) 所有的内角均相等；(ii) 1990 条边的长度是 $1^2, 2^2, 3^2, \cdots, 1989^2, 1990^2$ 的一个排列。

[32.2] 设整数 $n>6$，$a_1, a_2, \cdots, a_k$ 是所有小于 n 且与 n 互素的正整数。证明：如果

$$a_2-a_1=a_3-a_2=\cdots=a_k-a_{k-1}>0,$$

则 n 或者是素数或者等于 2^s，整数 $s\geqslant3$。

[32.3] 设集合 $S=\{1,2,3,\cdots,280\}$。求最小的正整数 n，使得 S 的每个有 n 个元素的子集必含有 5 个两两互素的数。

[32.6][①] 已给实数 $a>1$，构造一个有界无穷数列$x_0, x_1, \cdots$，使得当 $i\neq j$ 时必有$|x_i-x_j|\geqslant|i-j|^{-a}$。

① 本题可改进为 $a\geqslant1$。

习题的提示与解答

第 一 章

习 题 一

1. 作变数替换：$n=m+k_0-1$。$P(n)=P(m+k_0-1)=P^*(m)$。对$P^*(m)$用§1定理1.

2. $P^*(m)$同第1题解答，对$P^*(m)$用§1定理4.

3. 设T^*是T中所有正整数组成的子集。对T^*用§1定理2.

4. 考虑集合$T^*=\{t-a+1; t\in T\}$。对T^*用§1定理2.

5. 考虑集合$M^*=\{-m; m\in M\}$。对M^*用第4题结论。

6. 考虑集合$T=\{k; a^k\leq n, k\in \boldsymbol{Z}\}$。对$T$用第5题的结论。

习 题 二

2. $a_0=-x_0(x_0^{n-1}+a_{n-1}x_0^{n-2}+\cdots+a_1)$。

3. 利用第2题。(i) 无；(ii) 无；(iii) 无；(iv) $x=1$, $x=2$, $x=-2$。

4. 不可能。因为$100\nmid 3x+6y$, $x,y\in \boldsymbol{Z}$。

5. $7\cdot 5+(-2)\cdot 17=1$。利用§2例3.

6. $1\cdot 5+(-2)\cdot 2=1$，所以$10|n$。$3\cdot 7+(-2)\cdot 10=1$，所以$70|n$。

7. $n^k-1=((n-1)+1)^k-1=A(n-1)^2+k(n-1)$，$A$为整数。

8. $1234=2\cdot 617$，素除数：2,617；正除数：1,2,617,1234。$2345=5\cdot 7\cdot 67$，素除数：5,7,67；正除数：1,5,7,35,67,335,469,2345。$34560=2^8\cdot 3^3\cdot 5$，素除数：2,3,5；正除

数：$2^{\alpha_1}\cdot 3^{\alpha_2}5^{\alpha_3}$，$0\leqslant\alpha_1\leqslant 8$，$0\leqslant\alpha_2\leqslant 3$，$0\leqslant\alpha_3\leqslant 1$。

9．(i) 若$n\neq 2^k$，则$n=a\cdot m$，$2\nmid m>1$。$2^n+1=(2^a)^m+1=(2^a+1)((2^a)^{m-1}-(2^a)^{m-2}+\cdots+1)$。

(ii) 若n为合数，则$n=a\cdot m$，$a>1$，$m>1$。$2^n-1=(2^a)^m-1=(2^a-1)((2^a)^{m-1}+\cdots+1)$。$2^{2^0}+1=3$，$2^{2^1}+1=5$，$2^{2^2}+1=17$，$2^{2^3}+1=257$。$2^2-1=3$，$2^3-1=7$，$2^5-1=31$，$2^7-1=127$。

10．$(K+1)!+2$，$(K+1)!+3$，…，$(K+1)!+(K+1)$。

11．$2n+1=(n+1)^2-n^2$。

12．$k+1$个相邻正整数$m,m+1,\cdots,m+k$之和为$(k+1)\cdot(2m+k)/2$。设$n=m+(m+1)+\cdots+(m+k)=(k+1)(2m+k)/2$。若$k\geqslant 2$，显见$n$是合数。这就证明了必要性。若奇数$n>1$是合数，则$n=n_1n_2$，$n_1\geqslant n_2\geqslant 3$，可取$m_0=n_1-(n_2-1)/2$，$k_0=n_2-1$，得$n=m_0+\cdots+(m_0+k_0)$，$n$可表为三个或三个以上相邻正整数之和。这就证明了充分性。

13．若n/p不是素数，则必有素因数p'满足：$p'\leqslant(n/p)^{1/2}$，$p'\geqslant p$。由此推出$p\leqslant n^{1/3}$。这和假设矛盾。

14．$p_1^3\leqslant p_1p_2p_3\leqslant n$。　$2p_2^2\leqslant p_1p_2p_3\leqslant n$。

15．见附表1。用不超过$\sqrt{300}$的素数：2,3,5,7,11,13,17去筛选。

16．设N是给定正整数。$p_{11},p_{12},\cdots,p_{1r}$表所有不超过$N^{1/3}$的素数，$p_{21},p_{22},\cdots,p_{2s}$表所有不超过$(N/2)^{1/2}$的素数。这样，由第14题知，任一整数$n$：$N^{1/3}(N/2)^{1/2}<n\leqslant N$，是三个或三个以上素数乘积的充要条件是$n$可被某一乘积$p_{1i}p_{2j}$整除。由此，即可提出以下方法：把满足$N^{1/3}(N/2)^{1/2}<n\leqslant N$的正整数$n$列出，依次把能被$p_{1i}p_{2j}$整除的数都删去($1\leqslant i\leqslant r$，$1\leqslant j\leqslant s$)，剩下的就是素数或两个素数的乘积。再补上不超过$N^{1/3}(N/2)^{1/2}$的素数及$p_{1i}p_{j}$，($1\leqslant i\leqslant r$，$1\leqslant j\leqslant t$)就得到了不超过$N$的素数及两个素数乘积的全体正整数。当$N=100$时，不超过$100^{1/3}$的素

数是2,3，不超过$50^{1/2}$的素数是：2,3,5,7；不超过$100^{1/3}\cdot 50^{1/2}$(<33)的素数是：2,3,5,7,11,13,17,19,23,29,31．这样，不超过$100^{1/3}\cdot 50^{1/2}$的素数及两个素数乘积的正整数是：

$2,3,2\cdot 2,5,2\cdot 3,7,3\cdot 3,2\cdot 5,11,13,2\cdot 7,3\cdot 5,17,19,$

$3\cdot 7,2\cdot 11,23,5\cdot 5,2\cdot 13,29,31.$

再列出满足$100^{1/3}50^{1/2}<n\leqslant 100$的整数，依次删去能被$2\cdot 2$，$2\cdot 3,2\cdot 5,2\cdot 7,3\cdot 3,3\cdot 5,3\cdot 7$整除的整数，剩下的就是其中的素数及两个素数的乘积：

33	34	35	~~36~~	37	38	39	~~40~~	41	~~42~~	43	~~44~~
~~45~~	46	47	~~48~~	49	~~50~~	51	~~52~~	53	~~54~~	55	~~56~~
57	58	59	~~60~~	61	62	~~63~~	~~64~~	65	~~66~~	67	~~68~~
69	~~70~~	71	~~72~~	73	74	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	82	83	~~84~~	85	86	87	~~88~~	89	~~90~~	91	~~92~~
93	94	95	~~96~~	97	~~98~~	~~99~~	~~100~~				

实际上，以下的方法可能更方便：先找出不超过N的全体素数，然后补上不超过两个素数的乘积p_1p_2，$p_1\leqslant p_2\leqslant N/p_1$．

17．当$m>n$时必有$F_n|2^{2^m}-1$．

18．用归纳法．

19．当$m>n$时必有$A_n|A_m-1$．

20．用归纳法．

21．$5!-1=7\cdot 17$．

22．(i) 对任意x，$P(x)$都是合数；(ii) $P(x_0)=\pm p$，p是素数，则$p|P(x_0+jp)$，$j\in\mathbf{Z}$．

23．直接验证．

24．设$1\leqslant a_1<a_2<a_3$．若$a_3|a_1+a_2$，$a_2|a_3-a_1$，$a_1|a_2+a_3$，则$a_3=a_1+a_2$，$a_2=2a_1$．所有的集合为$k=3$，$\{a_1,2a_1,3a_1\}$．

25．用反证法及不可约数的定义．

26. $a|by$，$n=(1-ax)n$，所以 $a|n$。

27. 用反证法及合数的定义。

28. 利用§2定理5，及当 $N\to\infty$ 时 $\sum_{n=1}^{N}1/n\to+\infty$。

29. (i) 利用 $1/n>\ln(1+1/n)$，及 $\ln(1-1/p)^{-1}=\ln(1+1/(p-1))<1/(p-1)$；(ii) $\sum_{p\leqslant N}\{1/(p-1)-1/p\}<1$。

30. (i) 利用§2定理5；(ii) 当 $1\leqslant a\leqslant N$ 时，(i) 中的 k，l 满足：$1\leqslant k\leqslant\sqrt{N}$，以及 l 可能取值的个数 $\leqslant 1+\binom{\pi(N)}{1}+\binom{\pi(N)}{2}+\cdots+\binom{\pi(N)}{\pi(N)}=2^{\pi(N)}$；由(ii)推出(iii)及(iv)。

习 题 三

2. 设相邻的 a 个整数是：$m,m+1,\cdots,m+a-1$，它们被 a 除后的最小非负余数分别是：$r_0,r_1,\cdots,r_{a-1}$，$0\leqslant r_j<a$。这样，$r_j=r_0+j$，当 $r_0+j<a$；$r_j=r_0+j-a$，当 $r_0+j\geqslant a$。由此推出要么只有 $a|m$，当 $r_0=0$；要么只有 $a|m+j_0$，$j_0=a-r_0$，当 $r_0\neq 0$。

4. (i) 若 $2\nmid a$，则必有 x,y 使 $2x+ay=1$；(ii) 若 $7\nmid a$，则必有 x,y 使 $7x+ay=1$；(iii) $14|2\cdot 7$。

5. 若 $a|A_1-A_2$，则 A_1 与 A_2 被 a 除后的各种形式的余数都相等。

6. 同上题。

7. (i)—(iv)利用§2例3，及第2题；(v)利用(iv)及§2例3；(vii)利用(vi)，$5|n^5-n$，及§2例3；(viii)类似(vii)；(ix)利用 $5|n^5-n$，$3|n^3-n$，推出存在整数 A 使得

$$n^5/5+n^3/3+7n/15=n/5+n/3+7n/15+A$$
$$=n+A.$$

8. 下表列出了绝对最小余数

	3	4	8	10
n^2	{0,1}	{0,1}	{0,1,4}	{-4,-1,0,1,4,5}
n^3	{-1,0,1}	{-1,0,1}	{-3,-1,0,1,3}	{-4,-3,-2,-1,0,1,2,3,4,5}
n^4	{0,1}	{0,1}	{0,1}	{-4,0,1,5}
n^5	{-1,0,1}	{-1,0,1}	{-3,-1,0,1,3}	{-4,-3,-2,-1,0,1,2,3,4,5}

9. (i),(ii),(iii)利用§3定理1及第5题；(iv)由(ii)及(iii)推出。

11. (i) $j=0$; (ii) $j=1$; (iii) $j=8$.

12. $s=7$, $j_i=1+(i-1)3$, $1\leqslant i\leqslant 7$. 一般的，$s=b/a$, $j_i=j+(i-1)a$, $1\leqslant i\leqslant b/a$.

15. 利用第14题及证明§2定理7的方法。

16. (d) $1535625=3^3\cdot 5^4\cdot 7\cdot 13$;

$1158066=2\cdot 3^2\cdot 7^2\cdot 13\cdot 101$;

$82798848=2^8\cdot 3^5\cdot 11^3$;

$81057226635000=2^3\cdot 3^3\cdot 5^4\cdot 7^3\cdot 11^2\cdot 17\cdot 23\cdot 37$.

17. $7|n\Longleftrightarrow 7|2n$.

18. 利用§3定理1.

21. 利用第20题(i)，找一整数与和$1+1/2+\cdots+1/n$之积不是整数。

22. 利用第20题(ii)，及上题的方法。

23. 若$a_1=2^{r_1}m_1<a_2=2^{r_1}m_2$, $2\nmid m_1$, $2\nmid m_2$, 则必有$a_1<a<a_2$, $a=2^r m$, $2\nmid m$, $r>r_1$.

24. 利用上题，及第21题的证法。

25. 设$m\geqslant 1$, $r\geqslant 1$, $m+(m+1)+\cdots+(m+r)=(r+1)\cdot(2m+r)/2=n$. $r+1$和$2m+r$的奇偶性相反，这就证明了必要性。当$n=2^k\cdot n'$, $2\nmid n'>1$时，若$2^{k+1}>n'$, 取$r=n'-1$,

$2m=2^{k+1}-r$；若 $2^{k+1}<n'$，取 $r=2^{k+1}-1$，$2m=n'-r$．就证明了充分性。

27．分 $a<b$，$a\geqslant b$ 两种情形．$a<b$ 时，仅当 $a=1$，$b=2$ 时才可能有 $2^b-1|2^a+1$；$a\geqslant b$ 时，设 $a=qb+r$，$0\leqslant r<b$．易证 $2^b-1|2^a+1\Longleftrightarrow 2^b-1|2^r+1$。

28．仿照§3例5的证法．

29．(i) 3；(ii) 5；(iii) 1,2,4；1,2,－3；(iv) 1,3,9,5,4；1,3,－2,5,4。

30．(i) 找出 3^d 被13除后，可能取到的绝对最小余数；

(ii) 把(i)中的 3^d 换成 4^d．

31．参看§3结束时的讨论．

32．证明：$2^0,2^1,\cdots,2^{d_0-1}$ 被 a 除后所得的最小非负余数各不相同，而任一 2^k 被 a 除后所得的最小非负余数必和以上的 d_0 个中的一个相同。

习　题　四（Ⅰ）

1．(i) $\mathscr{D}(72,-60)=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\}$，$(72,-60)=12$；

(ii) $\mathscr{D}(-120,28)=\{\pm1,\pm2,\pm4\}$，$(-120,28)=4$；

(iii) $\mathscr{D}(168,-180,495)=\{\pm1,\pm3\}$，$(168,-180,495)=3$．

2．$2\cdot3\cdot5=30$，$2\cdot3\cdot7=42$，$2\cdot5\cdot7=70$，$3\cdot5\cdot7=105$．

3．(i) $\mathscr{D}(a,b,c)\subseteq\mathscr{D}(a,b)$，$\mathscr{L}(a,b,c)\supseteq\mathscr{L}(a,b)$；(ii) $\mathscr{L}(a,c)\supseteq\mathscr{L}(b,c)$，$\mathscr{D}(a,c)\subseteq\mathscr{L}(b,c)$；(iii) 及 (iv) $\mathscr{D}(a,b)=\mathscr{D}(ax+by,au+bv)$．

4．$d|c$，$d|a\Longrightarrow d|a+b$，$d|a\Longrightarrow d|b$，$d|a\Longrightarrow d=\pm1$，所以 $(c,a)=1$．同样证 $(c,b)=1$．或用第3题(ii)及 $(a,b)=(a,a+b)$．

5．$(n!+1,(n+1)!+1)=(n!+1,-n)=(1,-n)=1$．

6．(i) $(2t+1,2t-1)=(2t+1,-2)=(1,-2)=1$；

(ii) $(2n,2(n-1))=(2n,2)=2$；

(iii) $(kn,k(n+2))=(kn,2k)$。当 $n=2a$ 时，$(kn,2k)=(2ak,2k)=2k$；当 $n=2a+1$ 时，$(kn,2k)=(2ak+k,2k)=(k,2k)=k$；

(iv) $(n-1,n^2+n+1)=(n-1,2n+1)=(n-1,3)=3$，当 $n=3k+1$；$=1$，当 $n=3k-1,3k$.

7．$[a,b]\geqslant a\geqslant(a,b)$，$[a,b]\geqslant b\geqslant(a,b)$，所以，$a=b=(a,b)=[a,b]$。

8．$a=4k_1+2$，$b=4k_2+2$。

9．必可解出 $m=xu+yv$，$n=su+tv$，x,y,s,t 为整数．再利用第 3 题(iv)。

10．(i) 由 §2 例 3 知，若 $a|l$，$b|l$，则 $ab|l$；(ii) 若 $d|ac$，$d|b$，则 $d|acx+byc=c$。

11．必有整数 x,y 使 $2^kx+by=1$。

12．(i) 充分性：设 $l=cg$，取 $x=g$，$y=cg$；(ii) 充分性：设 $l=dg^2$，取 $x=g$，$y=dg$。

13．$(a/10,b/10)=1$，$[a/10,b/10]=10$．$a/10,b/10$ 仅可能取值 1,2,5,10，且满足上述条件．故得下表

$a/10$	1	10	2	5
$b/10$	10	1	5	2

14．{10,10,10}，{10,10,5}，{10,10,2}，{10,10,1}，{5,5,2}，{2,2,5}，{1,1,10}．{10,5,2}，{10,5,1}，{10,2,1}，{5,2,1}，以及它们的轮换。

15．$(a/10,b/10,c/10)=1$，$[a/10,b/10,c/10]=10$．$a/10$，

$b/10$, $c/10$ 仅可能取值 1,2,5,10 并满足上述两条件。有三种可能情形 (i) $a/10=b/10=c/10$，这不可能；(ii) 三个中有两个相等，由条件知另一个唯一确定，它们是 {10,10,1}，{5,5,2}，{2,2,5}，{1,1,10}，以及改变次序，共有 3·4 = 12 组解；(iii) 三个两两不等，任取三个不等的均可，它们是 {10,5,2}，{10,5,1}，{10,2,1}，{5,2,1} 及改变次序，共有 6·4 = 24 组解。把每个数都乘10就是原问题的解，共有36组解。

16. (i) $[198,252]=2[99,126]=18[11,14]=2^2\cdot 3^2\cdot 7\cdot 11$，最后一步用到了第10题(i)；(ii) $[482,1687]=241[2,7]=2\cdot 7\cdot 241$。

17. $a_1,2a_1,3a_1,4a_1,\cdots$ 中第一个能被 $a_2,\cdots$，及 a_k 都整除的数。

18. (ii) $(d,n)=1\iff(n-d,n)=1$。设 $d_1,\cdots,d_r$ 是小于 $n/2$ 且和 n 既约全部正整数，那么，$d_1,\cdots,d_r$，$n-d_r,\cdots,n-d_1$ 是不超过 n 且和 n 既约的全部正整数，这里 $n\geqslant 3$；

(iii) 由素数定义推出。

习 题 四 (Ⅱ)

1. $a=pa_1$，$b=p^2b_1$，$(a_1,p)=(b_1,p)=1$。$(ab,p^4)=p^3(a_1\cdot b_1,p)=p^3$。$(a+b,p^4)=p(a_1+pb_1,p^3)=p$。

2. $a=pa_1$，$b=pb_1$，$(a_1,b_1)=1$。$(a^2,b)=p(pa_1^2,b_1)=p(p,b_1)=p,p^2$。

   $(a^3,b)=p(a_1^3p^2,b_1)=p(p^2,b_1)=p,p^2,p^3$。

   $(a^2,b^3)=p^2(a_1^2,pb_1^3)=p^2(a_1,p)=p^2,p^3$。

3. (i) 不成立。如 $a=b=1$，$c=2$；

(ii) 成立。$(a,b,c)=((a,b),c)=((a,c),c)=(a,c)=(a,b)$；

(iii) 不成立。$d=4$，$a=4$，$b=2$；

(iv) 成立。因为 $a^4\mid b^4$，利用例 5 或例 6；

(v) 不成立。$a=8$，$b=4$；

(vi) 成立。见例 5 或例 6；

(vii) 成立。$[a^2,b^2]=a^2b^2/(a^2,b^2)=ab\cdot ab/(a,b)^2$，最后一步用到了例 6；

(viii) 成立。利用(vii)；

(ix) 成立。利用例 6。$(a^2,ab,b^2)=((a^2,b^2),ab)=((a,b)^2,ab)=(a,b)^2=(a^2,b^2)$；

(x) 成立。$(a,b,c)=(a,b,a,c)=((a,b),(a,c))$；

(xi) 不成立。$d=5$，$a=2$；

(xii) 成立。$a^4-1=(a^2-1)(a^2-1)$。

4. 利用例 5。

5. 设 $x_0=d/c$，$(c,d)=1$。则 $c|d$。

6. 用归纳法证提示中的结论，要利用

$$\cos(2m+1)\alpha=\cos(2m-1)\alpha\cdot\cos 2\alpha$$
$$-2\cos\alpha(\cos(2m-2)\alpha-\cos 2m\alpha)。$$

以及 $2\nmid n$ 时 $f_n(x)$的常数项为零；$2|n$ 时，$f_n(x)$的常数项为 ± 2。再利用上题。

7. $a=(da,dab/n)$，$a|dab/n$，所以 $n|db$。因而有 $a=(da,a(db)/n)=a(d,db/n)$，$(d,db/n)=1$。即$d(n,b)=n$。由$n\nmid b$，$n|db$ 推出 $d>1$。由 $n|ab$，$n\nmid a$ 推出$(n,b)>1$。由此及 $d(n,b)=n$ 推出 $d<n$。这结论表明有所说性质的 n 一定不是素数。

8. (i) $(d,ab)=(d,a)(d/(d,a),ba/(d,a))=(d,a)(d/(d,a),b)=(d,a)(d,b)$；(ii) 利用(i)。

9. $\mathscr{L}(a_1,a_2,\cdots,a_n)=\mathscr{L}([a_1,a_2],a_3,\cdots,a_n)=\mathscr{L}([a_1,\cdots,a_r],[a_{r+1},\cdots,a_n])$。

10. (i) $[a,b,c]=[[a,b],c]=[ab/(a,b),c]=abc/(ab,(a,b)c)$；

(ii) 由条件可得$(ab,bc,ca)=1$。用(i)。

11. 原式等价于

$$(a,b)(b,c)(c,a)=(a(a,b)(b,c),b(b,c)\cdot(c,a),c(c,a)(a,b)).$$

上式右边$=(a^2b,b^2a,abc,b^2c,c^2b,abc,c^2a,a^2c,abc)$。而左边$=(b(a,b),c(a,b))(c,a)=(ab,b^2,ca,cb)(c,a)=(abc,a^2b,a^2c,b^2a,b^2c,c^2b,c^2a)$。所以相等。

12. 上题第一式的右边$=(a,b,c)(ab,bc,ca)$。

13. $[(a,b),(a,c)]=(a,b)(a,c)/((a,b),(a,c))=(a,b)(a,c)/(a,b,c)$。$(a,[b,c])=(a,bc/(b,c))=(ab,bc,ca)/(b,c)$。再利用上题。

14. $[a,(b,c)]=a(b,c)/(a,b,c)$。$([a,b],[a,c])=(ab/(a,b),ac/(a,c))=a(ab,bc,ca)/(a,b,c)$。再利用第12题。

15. (i) 利用第13, 14题。$([a,b],[b,c],[c,a])=[([a,b],[b,c],c),([a,b],[b,c],a)]=[(c,[a,b]),(a,[b,c])]=[(a,b),(b,c),(c,a)]$;

(ii) 利用第10题(i)及第12题。

16. 利用例3。

18. (i) $(a,p^k)=1\Longleftrightarrow p\nmid a$。$1\leqslant a\leqslant p^k$中恰有$p^{k-1}$个$a$可被$p$整除;(ii) 利用例3,及(i)。

19. 利用第13题,及定理11。

20. 用归纳法证第一部份。其余同上题。

21. 显见只要考虑$2\nmid m$.设m的最小素因数是p,必有$p>2$。因此,$p|2^m-1$,$p|2^{p-1}-1$,进而有$p|2^{(m,p-1)}-1$。由p是m的最小素因数知,$(m,p-1)=1$,推出$p|1$,矛盾。

22. 不妨设$(a_n,\cdots,a_0)=(b_m,\cdots,b_0)=1$。用反证法。若$d=(c_{m+n},\cdots,c_0)>1$,则有素数$p|d$。设$i_0,j_0$分别是$p\nmid a_i,p\nmid b_j$的最大指标,即$p|a_i$,$i>i_0$,$p|b_j$,$j>j_0$。我们有$c_{i_0+j_0}=\sum\limits_{i+j=i_0+j_0}a_ib_j$。因此,推出$p|a_{i_0}b_{j_0}$,这和假设矛盾。

23. 设 c 是 m 的最大正除数使得 $(c,a)=1$，证明 $(a+bc,m)=1$。设 $d=(a+bc,m)$，由 $(a,bc)=1$，$d|a+bc$ 推出 $(d,a)=(d,bc)=1$，由此及 $d|m$，$c|m$ 推出 $dc|m$。由于 $(a,dc)=1$，所以由 c 的最大性推出 $d=1$。

24. 不妨设 $(a,b)=1$，$a>b$。若 $a^n-b^n|a^n+b^n$，则 $a^n-b^n|2$。

25. $(a^n-b^n)/(a-b)=na^{n-1}+A(a-b)=nb^{n-1}+B(a-b)$，$A,B$ 为两整数。所以 $((a^n-b^n)/(a-b),a-b)=(na^{n-1},a-b)=(nb^{n-1},a-b)=(na^{n-1},nb^{n-1},a-b)=(n(a,b)^{n-1},a-b)$。

26. (i) 不一定。可直接验证 $341=11\cdot31=n$ 就满足；

(ii) 设 $2^n-2=nk$。$2^{2^n-1}-2=2(2^{nk}-1)=2A(2^n-1)$；

(iii) $161038=2\cdot73\cdot1103$，$161038-1=3^2\cdot29\cdot617$，$73|2^9-1$，$1103|2^{29}-1$。

27. (i) $31\nmid11^{341}-1$。(ii) 设 $n=q_1\cdots q_k$，$q_1,\cdots,q_k$ 是两两不同的素数。若 $q_i-1|n-1$，$1\leqslant i\leqslant k$，则 n 是绝对伪素数。由此推出 $561=3\cdot11\cdot17$ 是绝对伪素数及(ii)。

28. 用归纳法证 $3^k|2^{3^k}+1$，$k=1,2,\cdots$。

29. (i) $m|2^m+2\Longleftrightarrow2^{n-1}+1|2^{2^n+1}+1=2^{k(n-1)}+1$，$k$ 是奇数。$m-1|2^m+1\Longleftrightarrow2^n+1|2^{2^n+2}+1=2^{hn}+1$，由于 n 一定是偶数，所以 h 是奇数；

(ii) $n=2$ 满足(i)中的两个条件。

30. $n=2p$，p 是奇素数，都满足。

习　题　四（Ⅲ）

2. 存在 x_0,y_0 使 $bx_0=cy_0+1$。$x_0^n\cdot a(a+b)\cdots(a+(n-1)b)=ax_0(ax_0+1)\cdots(ax_0+(n-1))+cA$，$A$ 为一整数。由此及 $n!|ax_0(ax_0+1)\cdots(ax_0+n-1)$，$c|n!$，$(c,x_0)=1$ 即得所要结论。

3. 若存在 $(a_s,a_t)=1$，则结论成立。若对任意的 s,t，总有 $(a_s,a_t)>1$，考虑 $d_i=(a_1,a_i)$，$i>1$。$d_i|a_1$，所以 $d_i>1$ 只取

有限多个值。因而，必有无穷子叙列 $a_{i_1} < a_{i_2} < \cdots$，使 $(a_1, a_{i_j}) = d$，$j = 1,2,\cdots$。这样，a_{i_j} 均可表为 a_1, a_{i_1} 的整系数线性组合，$j = 1,2,\cdots$。

4．$[d/2]+1$。

5．用例 9 的方法。

6．(i) 若 $a/b = 0.a_1a_2\cdots a_ka_1a_2\cdots a_k\cdots$ 是纯循环小数①，则 $a/b = a_1\cdots a_k/(10^k-1)$，所以 $(b,10)=1$。反之，若 $(b,10)=1$，则必有 k 使 $b \mid 10^k-1$。因此 $a/b = a\cdot A/(10^k-1) = a_1\cdots a_k/(10^k-1)$，即 a/b 是纯循环小数；

(ii) 由上面(i)的论证就可推出。

7．(iv) $10^{\gamma}(a/b) = m + a_1/b_1$，$0 < a_1 < b_1$。再利用上题。

习　题　五

1．(i) $3587 = 1819 + 1768$，$1819 = 1768 + 51$，$1768 = 34 \cdot 51 + 34$，$51 = 1 \cdot 34 + 17$，$34 = 2 \cdot 17$。所以 $(3587,1819) = 17$。$17 = 51 - 34 = 51 - (1768 - 34 \cdot 51) = 35 \cdot 51 - 1768 = 35(1819 - 1768) - 1768 = 35\cdot 1819 - 36 \cdot 1768 = 35 \cdot 1819 - 36(3587 - 1819) = -36 \cdot 3587 + 71 \cdot 1819$；

(ii) $(2947,3997) = 7 = -87 \cdot 3997 + 118 \cdot 2947$；

(iii) $(-1109, 4999) = 1 = 522 \cdot 4999 + 2353 \cdot (-1109)$；

(iv) $(15,21) = 3 = 3 \cdot 15 - 2 \cdot 21$，$(3,-35) = 1 = 3 \cdot 12 - 35$。所以，$(15,21,-35) = 1 = 12(3 \cdot 15 - 2 \cdot 21) - 35 = 36 \cdot 15 - 24 \cdot 21 + (-35)$；

(v) $(210,-330) = 30(7,-11) = 30$，$1 = -3\cdot 7 - 2\cdot(-11)$，$30 = -3 \cdot 210 - 2 \cdot (-330)$。$(30,1155) = 15(2,77) = 15$，$15 = -38 \cdot 30 + 1155$。所以，$(210,-330,1155) = 15 = 38(3 \cdot 210 + 2 \cdot (-330)) + 1155 = 114 \cdot 210 + 76 \cdot (-330) + 1155$。

① 这里的 $a_1a_2\cdots a_k$ 为表数的十进位表示，不是乘积。

2. 设$d=(m,n)$。$A=a^d-b^d$，$B=(a^m-b^m,a^n-b^n)$。显见，$A|B$，不妨设 $d=mx-ny$，$x>0$，$y>0$（必要时 m 和 n 可交换位置）。

$$a^{mx}=a^{ny}(A+b^d),$$
$$a^{mx}-b^{mx}=b^d(a^{ny}-b^{ny})+Aa^{ny},$$

所以，$B|Aa^{ny}$，由此及$(a,b)=1$ 推出 $B|A$。

8. 由 b_j 的递推公式证明：当 $k\geqslant1$ 时，$b_k\geqslant2^{(k+1)/2}$。

9. 由 c_j 的递推公式估计 c_h 的下界。

10. 对 k 用归纳法，通过依次比较 u_j,v_j 的关系，找出规律。

11. $q|2^{q-1}-1$。$q|2^{(p,q-1)}-1$。所以 $p|q-1$。由此及 q 是奇数推出 $q=2kp+1$。

12. $2^{11}-1$ 的素因数必为 $q=22k+1$。以 $q=23$ 试除得 $2^{11}-1=23\cdot89$。$2^{23}-1$ 的素因数 q 必为$46k+1$。$(2^{23}-1)^{1/2}<423$，以 47，139，277 等试除得 $2^{23}-1=47\cdot178481$。

13. 2^p-1 用二进位表示恰好是 p 个 1，即 11…11，共 p 位。

习 题 六

1. 推论 3。

2. 若 $p^\alpha\|g$，则 $p^{2\alpha}|abcd$。因而 p^α 至少整除 ac,bd 中的一个，由此及 $p^\alpha|ac+bd$ 即得 $p^\alpha|ac$，$p^\alpha|bd$。

3. 利用推论 5 或例 1 中的证法。

4. 利用第 1 题方法。设 $p^\alpha\|n$。分情形：(i) $p|a$，(ii) $p\nmid a$，$p|a-b$；(iii) $p\nmid a$，$p\nmid a-b$。

5. $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$p_1<\cdots<p_s$。$\tau(n)=(\alpha_1+1)\cdots(\alpha_s+1)=6$。必有 $\alpha_1=1$，$\alpha_2=2$；或 $\alpha_1=2$，$\alpha_2=1$。所以最小$n=2^2\cdot3^1=12$。

6. (i) 分别为 $a=2,1,12,24$，相应的解是：$\sigma(1)=1$，$\sigma(6)=\sigma(11)=12$；$\sigma(14)=\sigma(15)=\sigma(23)=24$。要利用以下结论：当

$r\geqslant3$时$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3})\geqslant72$，$r\leqslant2$时仅有以上的解；

(ii) $a=3^k(k\geqslant2)$时，$\sigma(n)=a$ 均无解。

7．利用§6式(7)，式(8)证．或利用定义证。

8．同第7题。证(ii)时，注意 $\prod\limits_{d\mid n}d=\prod\limits_{d\mid n}(d/n)$。

9．利用式(7)。

10．$\sigma_t(n)=\prod\limits_{j=1}^{s}(p_j^{t(\alpha_j+1)}-1)/(p_j^t-1)$，$n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$。

11．利用式(2)。

12．6，28。

15．直接求 $2^{k-1}(2^k-1)$的除数和。

16．证明必有 $k=1$。

17．设 $m=2^{r-1}m_1$，$2\nmid m_1$，$r>1$．$2m=\sigma(m)=(2^r-1)\sigma(m_1)$。设 $\sigma(m_1)=m_1+k$，得$m_1=(2^r-1)k$。利用上题。

18．利用第9题。

19．利用推论3，推论4，及组合公式。

20．同上题方法

21．设 $n=x^2-y^2(x>y\geqslant0)$的表法个数为T．由 $n=(x-y)\cdot(x+y)$，$x+y\geqslant x-y$ 知，$T=n$ 的不超过$\sqrt{n}$的正除数个数。

22．若 $\log_2 10=a/b$，$(a,b)=1$，$a\geqslant1,b\geqslant1$，$2^a=2^b5^b$。这不可能。

习　题　八

1．$b/a=[b/a]+\{b/a\}$，$b=[b/a]a+\{b/a\}a$，这给出了带余数除法(§3定理1)的一个新证明。

2．$b/a=2b/a-b/a=[2b/a]-[b/a]+\{2b/a\}-\{b/a\}$。并利用$-1/2\leqslant\{2x\}-\{x\}<1/2$。

3．$\{xy\}$与$\{x\}\{y\}$之间大于、等于、小于均可能出现。

4．原式等价于$[1/2+\{x\}]=[2\{x\}]$。然后对$\{x\}$分情形讨

论。

5．不妨设 $0\leqslant x<1$．必有整数 k，$0\leqslant k\leqslant n-1$，使 $k/n\leqslant x<(k+1)/n$．这样，易证等式两边均等于 k，第 4 题是本题的特例。

6．用带余数除法。

7．利用定理 1 的(iv)和(v)。

9．(i) 利用第 4 题，定理1(iv)．当 $\alpha=\beta=1/4$ 时第二个不等式不成立；

(ii) 充分性即(i)．当 $m<n$ 时，取 $\alpha=\beta=1/(m+n+1)$，不等式就不成立；当 $m>n$ 时，设 $m=kn+r$．若 $r=0$，则取 $\alpha=\beta=1/(2n)$，当 $2\mid k$；取 $\alpha=\beta=(k-1)/(kn)$，当 $2\nmid k$．若 $r>0$，取 $\alpha=\beta=k/m$。

10．(i) 所有整数 x；(ii) 满足 $2\{x\}<1$ 的实数 x；(iii) $1\leqslant x<12/11$；(iv) $10/11\leqslant x<1$；(v) 原式等价于 $2[x-1/2]=[2(x-1/2)]$；由(ii) 知是满足 $2\{x-1/2\}<1$的实数 x，即满足$1/2\leqslant\{x\}<1$ 的实数 x。

11．利用定理1(iv)。

12．利用$\{x\}$的性质，包括上题。

13．(i) 先证明

$$[(1+\sqrt{3})^{2m+1}]=(\sqrt{3}+1)^{2m+1}-(\sqrt{3}-1)^{2m+1},$$

$$(\sqrt{3}+1)^{2m+3}-(\sqrt{3}-1)^{2m+3}=8\{(\sqrt{3}+1)^{2m+1}$$
$$-(\sqrt{3}-1)^{2m+1}\}-4\{(\sqrt{3}+1)^{2m-1}-(\sqrt{3}-1)^{2m-1}\},$$

再利用归纳法证；(ii) 用反证法。若结论不成立，则有正整数K满足 $\sqrt{n}+\sqrt{n+1}<K\leqslant\sqrt{n}+\sqrt{n+2}$．这等价于 $n+1<(K-\sqrt{n})^2\leqslant n+2$及$K>2\sqrt{n}$．由此推出必有$K^2=4n+3$．这不可能。举例说明$[\sqrt[3]{n}+\sqrt[3]{n+1}]=[\sqrt[3]{n}+\sqrt[3]{n+2}]$就不一定成立。

14．数列$[\theta],[2\theta],\cdots,[n\theta]$恰好在$[n\theta]+1$个整数，$0,1,2,\cdots,[n\theta]$中取值。

15．用例 1 的方法，并注意图形的对称性。

16．同上题方法。

17．用例1的方法，及图形的对称性。求M的近似公式时以C/s代$[C/s]$。由(i)得的近似公式为

$$C\sum_{1\leqslant s\leqslant C}1/s-[C]<M\leqslant C\sum_{1\leqslant s\leqslant C}1/s.$$

由（ii）得的近似公式为

$$2C\sum_{1\leqslant s\leqslant\sqrt{C}}1/s-C-2\sqrt{C}<M\leqslant 2C\sum_{1\leqslant s\leqslant\sqrt{C}}1/s-C+2\sqrt{C}-1.$$

用你知道的办法去计算公式中的级数的渐近公式。

18．用例1的方法，及图形的对称性。

19．$2^{616}\|623!$，$3^{308}\|623!$，$6^{308}\|623!$，$12^{308}\|623!$，

$70^{102}\|623!$

20．即求10整除120!的最高次幂，也就是5整除120!的最高次幂。所以有28个零。

21．不成立。

22．$2^{31}\cdot3^{14}\cdot5^{7}\cdot7^{4}\cdot11^{2}\cdot13^{2}\cdot17\cdot19\cdot23\cdot29\cdot31$.

23．（i）$p=2$时，$e=n+\sum\limits_{j}[n/2^{j}]$，$p>2$时，

$$e=\sum_{j}[n/p^{j}];$$

(ii) $p=2$时$f=0$，$p>2$时$f=\sum\limits_{j}([2n/p^{j}]-[n/p^{j}])$.

25．不妨设$p\neq0$。设$ap=c_1$，$bp=c_2$，推出$ac_2=bc_1$，再利用条件$(a,b)=1$即得$a|c_1,b|c_2$。

26．利用上题及例4。

28．利用第23题(i)及第27题。

29．要证对任一素数p，有

$$\sum_{j}[nm/p^{j}]\geqslant n\sum_{j}[m/p^{j}]+\sum_{j}[n/p^{j}].$$

设 $m=p^l c$，$p\nmid c$。当 $j\leqslant l$ 时，$[nm/p^j]=n[m/p^j]$；当 $j>l$ 时，设 $m=q_j p^j+r_j$，$0<r_j<p^j-1$。我们有

$$[nm/p^j]=nq_j+[nr_j/p_j]=n[m/p^j]+[n\{m/p^j\}].$$

由此及 $\{m/p^j\}=\{c/p^{j-l}\}\geqslant 1/p^{j-l}$ 推出

$$\sum_{j>l}[nm/p^j]\geqslant n\sum_{j>l}[m/p^j]+\sum_{j=1}^{\infty}[n/p^j].$$

合起来即得所要结果。本题用排列组合法证简单。

30．利用第 9 题(i)。

31．当 $n=p^k$，p 素数，最大公约数为 p；其它情形为 1．$n=p^k$ 的情形，证明 $p\left|\binom{n}{l}\right.$，$1\leqslant l\leqslant n-1$，及 $p\nmid\binom{n}{p^{k-1}}$．不然，用反证法，若最大公约数 $d>1$，设 $p|d$。由于 $d|n$，可设 $n=p^k n_1$，$p\nmid n_1>1$，证明：$p\nmid\binom{n}{p^k}$，推出矛盾。

32．设 $p^e\| n!$，由公式 $e=\sum_j[n/p^j]$ 知，当 $n<p$ 时，$e=0$；当 $p\leqslant n<p^2$ 时，$1\leqslant e<p$；当 $p^2\leqslant n<p^3$ 时，$p+1\leqslant e<p^2+p-2$；当 $p^3\leqslant n<p^4$ 时，$p^2+p+1\leqslant e<p^3+p^2+p-2$。这样可看出 $a=p$，$a=p^2+p-2$，p^2+p-1，p^2+p 都是满足要求的数。上述过程继续下去就可定出所有这样的 a．

34．利用习题六第 1 题的方法，分 $p|b$，$p\nmid b$ 两种情形，及应用习题四(Ⅲ)第 2 题。

35．(i) 先分别证 a_n 两两不等，b_n 也两两不等；

(ii) 再证对任意的 m,n，$a_m\neq b_n$。因 α 是正无理数，必有 $0<i<m-1$ 使 $i/m<\alpha<(i+1)/m$。然后用反证法证明：若有这样的 n 使 $a_m=b_n$，则必有 $n>i$，$n<i+1$，得出矛盾；

(iii) 证明当 α 是正无理数时，a_n,b_n 取到全部正整数。对任一正整数 K，必有唯一的 $m\geqslant 1$ 及 $n\geqslant 1$，使

$$(m-1)(1+\alpha)<K<m(1+\alpha),$$

$$(n-1)(1+\alpha^{-1})<K<n(1+\alpha^{-1})。$$

因而有

$$(m+n-2)(1+\alpha^{-1})<K(1+\alpha^{-1})<(m+n)(1+\alpha^{-1}),$$

推出 $K=m+n-1$。注意到 $m\alpha>n$ 或 $m\alpha<n$ 有且仅有一式成立，由以上讨论推出 $K<m+m\alpha<K+1$ 或$K<n+n\alpha^{-1}<K+1$有且仅有一式成立，即 $a_m=K$ 或 $b_n=K$ 有且仅有一式成立。以上证明了充分性。当 $\alpha=a/b$ 为有理数时，只要 $m=bt$，$n=at$ 就给出 $[m+m\alpha]=[n+n\alpha^{-1}]$，这就证明了必要性。

36．充分性的证明。显见 $\alpha>1$，$\beta>1$，且 α,β 中必有一个小于2．不妨设 $1<\alpha<2$。令 $\alpha=1+\lambda$，就得 $\beta=1+\lambda^{-1}$。这就化成了上题的形式。必要性的证明．(i) 必有 $\alpha>1$，$\beta>1$；(ii) 设N是任给的正整数，以 $f(N)$及 $g(N)$分别表示由$[\alpha x]$及$[\beta x]$表出的不超过N的正整数个数。我们有$[\alpha x]\leqslant N$，$1\leqslant x\leqslant f(N)$和 $\alpha(f(N)+1)\geqslant N+1$；$[\beta x]\leqslant N$，$1\leqslant x\leqslant g(N)$，和$\beta(g(N)+1)\geqslant N+1$；以及 $f(N)+g(N)=N$．进而得$N<(N+1)(\alpha^{-1}+\beta^{-1})\leqslant N+2$。由此及$N$的任意性推出 $\alpha^{-1}+\beta^{-1}=1$。若$\alpha=v/u$为有理数，则 $\beta=v/(v-u)$。这时$[\alpha uk]=[\beta(v-u)k]$($k$ 任意正整数）就出现重复表示的正整数。

第 二 章

习 题 一

1．(i) $x_1=2+5t$，$x_2=1-3t$；(ii) 无解。$(60,123)=3\nmid 25$；(iii) 无解．$43\mid(903,731)$，$43\nmid 1106$；(iv) $x_1=3+5t$，$x_2=1-3t$；(v) $x_1=1778+1969t$，$x_2=1266+1402t$。

2．(i) $x_1=7+s$，$x_2=-s+3t$，$x_3=s-2t$；

(ii) $x_1=1+4s+2t$，$x_2=-t$，$x_3=-1+3s$；

(iii) 令 $3x_1+5x_2=y_1$，$3x_3-2x_4=y_2$。原方程变为 $2y_1-7y_2=1$。$y_1=4+7s$，$y_2=1+2s$。进而得

$x_1=2y_1+5t=8+14s+5t,\qquad x_2=-y_1-3t=-4-7s-3t,$
$x_3=y_2+2u=1+2s+2u,\qquad x_4=y_2+3u=1+2s+3u.$

3．(i) 消去 x_1 得 $9x_2-23x_3=3$。$x_2=-15+23s$，$x_3=-6+9s$。进而得 $x_1+73s=55$。$x_1=-18+73t$，$s=1-t$。所以，$x_2=8-23t$，$x_3=3-9t$；

(ii) $x_1=3+7s$，$x_2=-1-3s$ 进而得 $29s+10x_3=-3$，$s=3+10t$，$x_3=-9-29t$。$x_1=24+70t$，$x_2=-10-30t$；

(iii) $x_2^2=2x_2(x_3-x_1)$。(a) $x_2=0$，$x_1=-x_3$；(b) $x_2\neq 0$。$x_1=3t$，$x_2=4t$，$x_3=5t$，$t\neq 0$；

(iv) $x_1=-1+6t$，$x_2=111-7t$，$x_3=-16+t$；

(v) $5x_2+20x_3=1$，无解；

(vi) 先得 $x_3+3x_4=150$，解出 $x_3=3t$，$x_4=50-t$，进而得 $x_2=50-3t$，$x_1=t$。

4．设解为 $x=x_0+bt$，$y=y_0-at$。相邻的两解(即对应于t，$t+1$)所给出的整点之间的距离等于$(a^2+b^2)^{1/2}$。

5．充分性显然。取 $t=0$ 得 $x_1=e$，$x_2=g$ 是解。进而，对任意的整数 t 有 $a_1ft+a_2ht=0$，因此，$a_1f+a_2h=0$。所以有 $a_1/(a_1,a_2)|h$，$a_2/(a_1,a_2)|f$。另一方面 $x_1=e+a_2/(a_1,a_2)$，$x_2=f-a_1/(a_1,a_2)$是一组解，所以必有t_1使$a_2/(a_1,a_2)=ft_1$，$-a_1/(a_1,a_2)=ht_1$。由此就推出余下的结论。

8．(i) $x_1=4+7t$，$x_2=3-5t$。$x_1=4$，$x_2=3$。

(ii) $x_1=-1000+97t$，$x_2=1000-96t$。无非负解、正解；

(iii) $x_1=3t$，$x_2=41-7t$。全部正解是由 $t=1,2,3,4,5$给出，非负解再加上 $t=0$。

(iv) $x_1=1$，$x_2=2$，$x_3=1$。

9．x、y、z 分别表大、中、小学生人数。$x+y+z=20$，$6x+4y+z=40$。$x=4$，$y=0$，$z=16$；$x=1$，$y=5$，$z=14$。

10．x,y,z 分别表 1元，2元，5元的张数。$x+y+z=50$，$x+2y+5z=100$。$x=36+3t$，$y=2-4t$，$z=12+t$，$t=0,-1,-2$，

$\cdots, -12$。

11. x, y, z 分别表甲，乙，丙的钱数。$x+y+z=100$, $18x+y+3z=300$。$x=10-2t$, $y=75-15t$, $z=15+17t$, $t=0,1,\cdots,5$。

12. 以 x, y 表黑、白瓜子的包数，黑瓜子每包 z 角。$x+y=12$, $xz+y(z+3)=99$, $y>x$。先解 $12z+3y=99$。最后得 $x=3$, $y=9$，黑瓜子每包 6 角。

13. 设降低后的价格为 u 角，甲以 5 角和 u 角卖出的鸡蛋数为 x_1, x_2，乙为 y_1, y_2。$x_1+x_2=40$, $y_1+y_2=30$。$5x_1+ux_2=5y_1+uy_2$。$u=3$，以及最多 15 元，最少 12 元。

14. $7x+10y=100$。甲班分 70 个，乙班 30 个。

15. (i) 设 $23/30=b_1/a_1+b_2/a_2+b_3/a_3$。$(a_1, a_2)=(a_2, a_3)=(a_3, a_1)=1$, $a_j\geqslant 2$, $(a_j, b_j)=1$。由 $30=2\cdot 3\cdot 5$ 知可设 $a_1=2$, $a_2=3$, $a_3=5$。$15b_1+10b_2+6b_3=23$。$23/30=1/2-1/3+3/5$。

(ii) $23/30=a_1/5+a_2/6$。$a_1=3, a_2=1$。两题均可有别的解，但 (i) 中的三个分母是唯一的。

16. 这堆椰子最少有 3121 个。五人依次拿到的椰子个数为 828, 703, 603, 523, 459，猴子吃了 5 个。

17. (i) $x_1=40, x_2=15, x_3=5$。 (ii) 25,2,4; 24,4,3; 23,6,2; 22,8,1。

20. $x_1=71, x_2=22$。显然 $6893<63\cdot 1100$，但仍有正解。

22. 设 x_1^0, x_2^0, x_3^0 为一组特解，任意一组解 x_1, x_2, x_3 必满足 $a_2a_3(x_1-x_1^0)+a_3a_1(x_2-x_2^0)+a_1a_2(x_3-x_3^0)=0$。因此，$a_1\mid x_1-x_1^0$, $a_2\mid x_2-x_2^0$, $a_3\mid x_3-x_3^0$，即有 $x_1=x_1^0+a_1t_1$, $x_2=x_2^0+a_2t_2$, $x_3=x_3^0+a_3t_3$, $t_1+t_2+t_3=0$。若有非负解，那么，当 x_2, x_3 取最小非负值时，x_1 的值必为非负。所以取 t_2, t_3 使 $0\leqslant x_2=x_2^0+a_2t_2\leqslant a_2-1$, $0\leqslant x_3=x_3^0+a_3t_3\leqslant a_3-1$，得到 $a_2a_3(x_1^0+a_1t_1)\geqslant c-2a_1a_2a_3+a_3a_1+a_1a_2$。由此就推出当 $c>2a_1a_2a_3-a_1a_2-a_2a_3-a_3a_1$ 时，$x_1>-1$，即必有非负解。当 $c=2a_1a_2a_3-a_1a_2-a_2a_3-a_3a_1$ 时，若有非负解

x_1, x_2, x_3，则 $a_2a_3(x_1+1)+a_3a_1(x_2+1)+a_1a_2(x_3+1)=2a_1a_2a_3$。由此推出 $a_1|x_1+1 \geqslant a_1$，$a_2|x_2+1 \geqslant a_2$，$a_3|x_3+1 \geqslant a_3$。这和上式矛盾。

23．$(1-y^{a_1})^{-1}\cdots(1-y^{a_k})^{-1}$ 的幂级数展开式中 y^n 的系数。要求正解个数时要讨论 $y^{a_1+\cdots+a_k}(1-y^{a_1})^{-1}\cdots(1-y^{a_k})^{-1}$。

习 题 二

1．例 1 中 $r \leqslant 6$ 就给出了 y 为偶的所要的全部本原解。由此及式(9)，式(10)就可得到 $|z| \leqslant 50$ 的全部解和正解。

2．(i) 本原的有 $\{15,8,17\}$，$\{15,112,113\}$，非本原的有：$\{15,36,39\}$，$\{15,20,25\}$，$\{9,12,15\}$；(ii)无本原的，非本原的有：$\{22,120,122\}$；(iii)无本原的，非本原的有：$\{14,48,50\}$，$\{30,40,50\}$，$\{50,120,130\}$，$\{50,624,626\}$。

3．(i) $2 \nmid n$ 或 $4|n$ 时有解；(ii) $2 \nmid n$ 或 $8|n$ 时有本原解。通过讨论 $n=n_1n_2$，$x-y=n_1$，$x+y=n_2$，$2|n_1+n_2$，得到方程的解。

5．(i) $1105 = 5 \cdot 13 \cdot 17$。$5 = 2^2+1^2$，$13 = 3^2+2^2$，$17^2 = 4^2 + 1^2$。进而利用第 4 题(i) 得：$5 \cdot 13 = 8^2+1^2 = 7^2+4^2$，$5 \cdot 17 = 9 + 2^2 = 7^2+6^2$，$13 \cdot 17 = 14^2+5^2 = 11^2+10^2$，$5 \cdot 13 \cdot 17 = 33^2+4^2 = 32^2+9^2 = 31^2+12^2 = 24^2+23^2$。由此，对 $z=1105$ 确定式(9)和(10)中的 k, r, s 就可得到全部要求的本原与非本原商高三角形。

6．利用第 3 题。

7．设 x, y, z 由式(6)及式(7)给出。边长为 dx，dy，dz 的商高三角形的面积 $A = d^2rs(r-s)(r+s)$。以 $A = 78,360$ 去试算，可知没有这样的三角形。

8．利用第 3 题。

9．必有 $2 \nmid x$，$2 \nmid z$，及 $2|y$。所以方程变为 $2(y/2)^2 = (z-x)/2 \cdot (z+x)/2$。然后，按定理 2 一样讨论。

10．x^2, y, z 是方程(1)的既约解。进而利用公式(6)，(7)，讨

论 $x^2=r^2-s^2$ 或 $x^2=2rs$ 的解。

11．$3|z+x$或$3|z-x$有且仅有一个成立，$(z-x,z+x)=1$或2，把方程写为 $y^2=(z+x)/3\cdot(z-x)$或 $y^2=(z+x)\cdot(z-x)/3$，然后仿照定理 2 一样讨论。

12．若 x,y,z 是正解，则 $x/(x,y),y/(x,y),xy/(z(x,y))$ 是方程(1)的本原解。

13．由推论 5 推出。

14．(i) 若有解 x_0,y_0,z_0，则必有一组两两互素的正解 x_1,y_1,z_1；

(ii) 设 x_1,y_1,z_1 是所有两两互素的正解中使得 y_1 为最小的。利用 $((z_0-x_0^2)/2,(z_0+x_0^2)/2)=1$，仿照定理 4 一样讨论(本题解法很多，也可设 z_1 是最小的)。

15．仿照定理 4 证。

16．利用定理 2，去推出矛盾。

17．由此题知，以上三题只要直接去证一个。

18．若有解，则利用定理 2 可推出第14题有 $xyz\neq0$ 的解。

19．直接仿照第14题证，或由第20题知可从定理 4 推出。

21．设$x=2l$，$y=2m$。$(z+w)(z-w)=2^2(l^2+m^2)$。因此必有 $z+w=2n$，$z-w=2(l^2+m^2)/n$，$n|l^2+m^2$。由此推出，x,y,z,w 有所说的形式。反过来，直接验证给出的都是解。

22．$x=(1+k^n)$，$y=k(1+k^n)$，$z=(1+k^n)$，k 任意整数。

23．$x=(1+k^n)^{n-2}$，$y=k(1+k^n)^{n-2}$，$z=(1+k^n)^{n-1}$，k 任意整数。

24．用反证法。若有解，则 $2\nmid x$，设 $x=2k+1$，得 $2k(k+1)=y^4$。所以必有(i) $2k=u^4$，$k+1=v^4$，或(ii) $k=u^4$，$2(k+1)=v^4$，$2\nmid uv$，$(u,v)=1$。若(i)成立，设 $u=2^r u_1$，得 $v^4=1+2^{4r-1}u_1^4$，$v^4+(2^{2r-1}u_1^2)^4=(1+2^{4r-2}u_1^4)^2$。但这和定理 4 矛盾。若(ii)成立，设 $v=2^r v_1$，得$u^4+1=2^{4r-1}v_1^4$，$u^4+(1-2^{4r-2}v_1^4)^2=(2^{2r-1}v_1^2)^4$，这和第15题矛盾。

25. 原方程等价于 $y^4 = x^4 + (y^2 - 1)^2$。由此及第15题就推出所要结论。

26. $(x-1)(x+1) = 8y^4$，必有(i) $x-1 = 2u^4, x+1 = 2^{4r+2}v^4$；或(ii) $x-1 = 2^{4r+2}u^4$，$x+1 = 2v^4$，$2 \nmid uv$，$(u,v) = 1$。类似第24题的讨论，并利用第25题。

第 三 章

习 题 一

3. $m \mid (a-b, c-d)$。

4. (i) 最小非负剩余：1,3；最小正剩余：1,3；绝对最小剩余：$-1, 1$。$p = 5, 3$。(ii) 最小非负剩余及最小正剩余系：1, 5；绝对最小剩余：$-1, 1$。$p = 7, 5$。(iii) 最小非负剩余及最小正剩余：1,7,11,13,17,19,23,29；绝对最小剩余：$\pm 1, \pm 7, \pm 11, \pm 13$。$p = 29, 31, 23, 7, 19, 11, 17, 13$。

7. (i) 不成立。$5^2 \equiv 7^2 \pmod 8$，$5 \not\equiv 7 \pmod 8$；(ii) 不成立。例如(i) $5 \not\equiv \pm 7 \pmod 8$；(iii) 不成立。$5 \equiv -3 \pmod 8$，$25 \not\equiv 9 \pmod{64}$；(iv) 成立。因为 $2 \mid a-b \Longrightarrow 2 \mid a+b$；(v) 成立。因为 $p \mid (a-b)(a+b)$，$p \nmid (a-b, a+b) \mid 2(a,b)$；(vi)成立。利用性质Ⅷ，设 $c = (a^k)^{-1} \bmod m$，$1 \equiv ca^k \equiv cb^k \pmod m$。$a \equiv ca^{k+1} \equiv cb^{k+1} \equiv b \pmod m$。

8. $1 + 2 + \cdots + (m-1) + m \equiv m + (1 + (m-1))$

$$+ (2 + (m-2)) + \cdots \equiv 0 \pmod m$$，当 $2 \nmid m$；$\equiv m/2 \not\equiv 0 \pmod m$，当 $2 \mid m$。

9. $1^3 + 2^3 + \cdots + (m-1)^3 + m^3 \equiv m^3 + (1 + (m-1)^3) + \cdots \equiv 0 \pmod m$，当 $2 \nmid m$；$\equiv (m/2)^3 \pmod m$，当 $2 \mid m$。当 $2 \nmid m$ 或 $4 \mid m$ 时成立，当 $2 \mid m$，$4 \nmid m$ 时不成立。

10. 0,1,3,5,6,8。

12. $n = d_1 d_2$，$2 \leqslant d_1, d_2 \leqslant n/2$。当 $d_1 \neq d_2$ 时显有 $(n-2)! \equiv 0 \pmod n$。当 $d_1 = d_2$ 时，由于 $n > 4$ 所以 $d_1 \geqslant 3$，$2 \leqslant d_1 < 2d_1 \leqslant$

$n-2$。因此，$(n-2)!\equiv 0 \pmod n$ 也成立。这就证明了必要性。充分性显然。

13．原式等价于 $9!+1\equiv 0 \pmod{71}$。

14．(i) 6；(ii) $2^{22}\equiv 4 \pmod{100}$。$2^{1000}\equiv 2^{100}\equiv 2^{20}\equiv 76 \pmod{100}$，76；(iii) $9^{10}\equiv(10-1)^{10}\equiv 1 \pmod{100}$，$9^{9}\equiv(10-1)^{9}\equiv 9 \pmod{10}$，所以，$9^{9^{9}}\equiv 9^{9}\equiv -11\equiv 89 \pmod{100}$，末两位数为89。$9^{9^{9^{9}}}\equiv 9^{89}\equiv 9^{9}\equiv 89 \pmod{100}$，末两位数也是89；(iv) 70；(v) 6。

15．(i) -2；(ii) -3。

17．(i) $n=4$；(ii) $n=9$。

18．$n=4k+1\equiv 2 \pmod 3$，$k=1$，$n=5$。

19．$n\equiv 0 \pmod 2 \Longleftrightarrow n\equiv 0,2,4,6,8$，或 $10 \pmod{12}$；$n\equiv 0 \pmod 3 \Longleftrightarrow n\equiv 0,3,6$，或 $9 \pmod{12}$；$n\equiv 1 \pmod 4 \Longleftrightarrow n\equiv 1,5$，或 $9 \pmod{12}$；$n\equiv 5 \pmod 6 \Longleftrightarrow n\equiv 5$ 或 $11 \pmod{12}$；以及 $n\equiv 7 \pmod{12}$ 本身。

20．同上题证法。

21．用例4的方法证。

22．若 a,b,c 满足要求，则对任意 $k\geqslant 1$，ka,kb,kc 也满足，所以，可先设 $(a,b,c)=1$，及 $1\leqslant a\leqslant b\leqslant c$。由此及 $c\mid a-b$ 推出 $a=b$，进而由 $a\mid c$ 及 $(a,b,c)=1$ 推出 $a=b=1$。所以，所有解为 $\{1,1,c\}$，c 为任意正整数。

23．类似上题，可先假定 $(a,b,c)=1, c>0$，及 $|a|\leqslant|b|\leqslant c$。推出必有 (i) $a=b$，(ii) $a-b=\pm c$，(iii) $a-b=\pm 2c$。这三种情形可分别得到 (i) $\{1,1,c\},\{-1,-1,c\}$；(ii) $\{1,-n,n+1\}$，$\{2,-(2n+1),2n+3\}$，n 为任意正整数；及 $\{-1,1,2\}$，$\{-1,2,3\}$；(iii) $\{1,-1,1\}$，$\{-1,1,1\}$。

24．由第一章§4例3(ii)推出。

25．第一部分利用多项式除法，用归纳法证明。由此推出第二部分中的各个结论，最后一个结论(d)要通过比较式(a)两边

x^{p-2}的系数推出。

26．设 $(x-1)\cdots(x-p+1)=x^{p-1}+s_1x^{p-2}+\cdots+s_{p-2}x+(p-1)!$。由此及第25题(a)，(c)推出 $p\mid(s_1,\cdots,s_{p-2})$。在上式中令$x=p$，由此即得 $p^2\mid s_{p-2}$，这就是要证的结论。

习 题 二（I）

2．(i) 1,11,3,13,5,15,7,17,9；(ii) 0,10,2,12,4,14,6,16,8；(iii) 由式(4)知不能；(iv) 由式(4)推出。

3．(i) 21,15,3,−3,12,6；(ii) (i)中的每个数加1；(iii) (i)中的每个数减1。

4．对任意 r 必有 h_r,k_r 使 $h_ra+k_rm=s-r$。

5．因 $j^2\equiv(m-j)^2(\bmod m)$。

6．利用式(5)。

7．利用鸽巢原理，必有两数属于同一剩余类。

8．当m是偶数时，以$1\bmod m$，$2\bmod m$为一组，$3\bmod m$，$4\bmod m$为一组，…，$(m-1)\bmod m$，$m\bmod m$为一组，把m个剩余类两两分组。这样，任取$[m/2]+1$个数，必有两个数在同一组中，所以结论成立。

当m为奇数时，以$1\bmod m$为单独一组，$2\bmod m$，$3\bmod m$为一组，…，$(m-1)\bmod m$，$m\bmod m$为一组，把m个剩余类分为$[m/2]+1$组。当有两数属于后面的$[m/2]$组的某一组时，结论成立。不然，必是一个数属于$1\bmod m$，及其它各组中各有一数。若结论不成立，则其它各数必是依次属于$3\bmod m$，$5\bmod m$，…，$(m-2)\bmod m$，$m\bmod m$。但属于$1\bmod m$和$m\bmod m$的两数之差属于$1\bmod m$。

9．(i) $1\bmod 5=\bigcup\limits_{0\leqslant r\leqslant 4}(1+5r)\bmod 15$；

(ii) $6\bmod 10=\bigcup\limits_{0\leqslant r\leqslant 11}(6+10r)\bmod 120$；

(iii) $6 \bmod 10 = \bigcup_{0 \leqslant r \leqslant 7} (6 + 10r) \bmod 80$.

10. (i) $\pm 1, \pm 3, 5$; (ii) $4, 9, 14, 19, 24, 29, 34, 39, 44$.

11. $(2n-1, n-2) = 1$，当$3 \nmid n-2$；$=3$，当$3 | n-2$。当$(2n-1, n-2) = 1$时，最少属于1个模$n-2$的剩余类；当$(2n-1, n-2) = 3$时，最少属于3个模$n-2$的剩余类，一般最少属于(K, m)个模m的剩余类。

15. 利用第14题。

18. 若$(a, d) > 1$则必有$(a, n) > 1$。此外，在d个相邻整数中与d不互素的数有$d - \phi(d)$个。所以，$n - \phi(n) \geqslant (n/d)(d - \phi(d))$。

19. 对素数$p > 3$必有$\phi(p) > \phi(p+1)$。$\phi(3) = \phi(4) = \phi(6)$。

20. $\phi(p_1 p_2)$等于$1, 2, \cdots, p_1 p_2$中与$p_1 p_2$既约的数，即不能被p_1或p_2整除的数的个数，即$p_1 p_2 - (p_1 + p_2 - 1)$。

21. 因为对给定的t，$tm+1, tm+2, \cdots, tm+m$中和m既约的数恰有$\phi(m)$个。

22. (i) $\phi(p_1 p_2 p_3)$是$1, 2, \cdots, p_1 p_2 p_3$中不能被$p_1, p_2$，或$p_3$整除的数的个数。被$p_1, p_2, p_3$整除的数分别有$p_2 p_3, p_3 p_1, p_1 p_2$个，其中被两个素数整除的数重复算了两次，被三个素数整除的数重复算了三次。被$p_1 p_2, p_2 p_3, p_3 p_1$整除的数分别有$p_3, p_2, p_1$个，其中被三个素数整除的数重复算了三次。而被$p_1 p_2 p_3$整除的有1个。因此，$\phi(p_1 p_2 p_3) = p_1 p_2 p_3 - p_2 p_3 - p_3 p_1 - p_1 p_2 + p_3 + p_2 + p_1 + 1 = (p_1 - 1)(p_2 - 1)(p_3 - 1)$。

(ii) 同样论证。这就是常用的组合数学中的容斥原理。

23. 由第21题知$1, 2, \cdots, p_1 \cdots p_{k-1} p_k$中与$p_1 \cdots p_{k-1}$既约的数有$p_k \phi(p_1 \cdots p_{k-1})$个，其中被$p_k$整除的数必为$a p_k$，$(a, p_1 \cdots p_{k-1}) = 1$，$1 \leqslant a \leqslant p_1 \cdots p_{k-1}$，所以恰有$\phi(p_1 \cdots p_{k-1})$。所以，$\phi(p_1 \cdots p_k) = (p_k - 1)\phi(p_1 \cdots p_{k-1})$。由此及归纳法即得所要结论。

24. 利用第21题（取$n = p_1 \cdots p_r$，$h = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}$）及第22题(ii)。

习 题 二（Ⅱ）

3. (i) 和式 $=\sum_{r=0}^{m-1}\left\{\frac{r}{m}\right\}=\sum_{r=0}^{m-1}\frac{r}{m}$；

(ii) 和式 $=\sum_{\substack{r=1\\(r,m)=1}}^{m}\frac{r}{m}$。

4. 利用定理10和 9 。

5. $r_j=7k_j$，$7k_j\equiv j \pmod 5$，$k_j\equiv 3j \pmod 5$。只要取 k_j 是模23的完全剩余系且满足 $k_j\equiv 3j \pmod 5$。设 $k_j=j+23h_j$，得 $h_j\equiv -j \pmod 5$。任取 h_j 满足这条件，定出 k_j，最后得 r_j。

7. 取 $r_i=5i+4$，$1\leqslant i\leqslant 4$，$s_j=5+4j$，$1\leqslant j\leqslant 5$ 即可使(i)及(ii)都成立。

8. (i) 成立。取第 7 题给出的完全剩余系中的既约剩余系即可。

(ii) 不成立。因为这时必有 $(r_is_j,20)=1$。当 $\{r_i\}$ 是模 4 的既约剩余系时，对任一固定的 s_{j_0}，由 $(s_{j_0},4)=1$ 可推出 $\{r_i+s_{j_0}\}$ 中必有数和 4 不既约（利用式(9)）。但可以单独要求 r_i+s_j 是模20的既约剩余系。这只要取 $r_i=5i$，$s_j=4j$ 即可。

9. 仿照第 7 题。

10. 利用证明定理14的方法。其含意同第 9 题（推广到 k 个两两既约模的情形）。

习 题 三

1. (i) 只要 $3^2\nmid n$ 及 n 没有 $3k+1$ 形式的素因数；

(ii) 设 p 是 d 的最大素因数。若 $p\geqslant 3$，那么只要 $p^2\nmid n$ 及 n 没有 $pk+1$ 形式的素因数，就有 $p\nmid\phi(n)$，因而 $d\nmid\phi(n)$；若 $p=2$，则 $4\mid d$，那么，只要 n 是 $4k+3$ 形式的素数，就有 $4\nmid\phi(n)$。

2. 因为当 $n\to\infty$ 时，$\phi(n)\to\infty$。

3. (i) 用定理 1 (i)。$[m,n]$与 mn 有相同的素因数；(ii) 利用定理 1 的式(5)；(iii) 由(ii)推出。

4. $k=3$ 无解； $k=1$恰有两解：$\phi(2)=\phi(1)=1$，因为 $2|\phi(n), n\geqslant 3$； $k=2$恰有三解：$\phi(6)=\phi(4)=\phi(3)=2$，因为这时 n 只能有小于 5 的素因数； $k=4$恰有四解：$\phi(12)=\phi(10)=\phi(8)=\phi(5)=4$，因为这时 n 只能有小于 7 的素因数。（利用式(5)）。

5. 当 $\phi(n)=24$时，n 仅可能有2,3,5,7,13作为其素因数。设 $n=2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}13^{\alpha_5}$，可算出：$n=13\cdot 3, 13\cdot 3\cdot 2, 13\cdot 2^2, 7\cdot 5, 7\cdot 5\cdot 2, 7\cdot 3\cdot 2^2, 7\cdot 2^3, 5\cdot 3^2, 5\cdot 3^2\cdot 2, 3^2\cdot 2^3$。

6. (i) $2\nmid n$； (ii) $2|n, 3\nmid n$； (iii) $2\nmid n, 3\nmid n$。 在(ii), (iii)只要讨论 $n=2^\alpha 3^\beta\cdot m, (6,m)=1$。

7. $n=2^7, 2^6\cdot 3, 2^5\cdot 5, 2^4\cdot 3\cdot 5$； $2^3\cdot 17, 2^2\cdot 3\cdot 17, 2\cdot 5\cdot 17, 5\cdot 17$。

8. 即要从 $m\phi(m)=n\phi(n)$推出 $m=n$。 设 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, $n=p_1^{\beta_1}\cdots p_r^{\beta_r}$， $p_1>p_2>\cdots>p_r$， 利用式(5)依次证明：$\alpha_1=\beta_1$, $\alpha_2=\beta_2, \cdots$。

9. 可设$(a,b)=1$。 $m=a^k b^{k+1}, n=a^{k+1}b^k, k\geqslant 1$。

10. 若$2\nmid k$，则可取 $n=k$。若$2|k$，设 p_0 是最小素数使得 $p_0\nmid k$， 可取 $n=(p_0-1)k$。

11. 由第 3 题(ii)推出。

12. (i) 当 $p>2$ 时， $\phi(p^\alpha)=(p-1)p^{\alpha-1}>p^{\alpha/2}$， $\phi(2^\alpha)>2^{\alpha/2}/2$；

(ii) n为合数时必有素因数$p\leqslant\sqrt{n}$，p 的倍数均不和n既约。

13. $n=1, 2^\alpha\cdot 3^\beta, \alpha\geqslant 1, \beta\geqslant 0$。

14. 利用§1性质Ⅸ，§3定理3，式(17)，及例2。

15. (i) 若 $p_i|a$，则 $p_i^{\alpha_i}|a^{\alpha+\phi(m)}-a^\alpha$； 若 $p_i\nmid a$，则 $p_i^{\alpha_i}|a^{\phi(p_i^{\alpha_i})}-1$，进而 $p_i^{\alpha_i}|a^{\phi(m)}-1$； (ii) 若 $p_i\nmid a$，则由 (i) 知 $p_i^{\alpha_i}|a^{\phi(m)}-1$，进而有 $p_i^{\alpha_i}|a^{m-\phi(m)}(a^{\phi(m)}-1)=a^m-a^{m-\phi(m)}$；若 $p_i|a$，由$m-\phi(m)\geqslant p_i^{\alpha_i-1}\geqslant\alpha_i$（这可由习题二(Ⅰ)第 18 题或§3

式(5)推出),也得到$p_i^{\alpha_i} | a^m - a^{m-\phi(m)}$; (iii)从(i)的讨论可推出。

16. 由§1性质Ⅸ及§3定理3推出。

17. 设 $f(x) = a_n x^n + \cdots + a_0$. $(f(x))^p = (a_n x^n)^p + (a_{n-1}x^{n-1})^p + \cdots + a_0^p + p \cdot h_1(x)$, $h_1(x)$是整系数多项。进而由Fermat 小定理得 $(f(x))^p = a_n (x^p)^n + a_{n-1}(x^p)^{n-1} + \cdots + a_0 + ph_2(x) = f(x^p) + p \cdot h_2(x)$。$h_2(x)$是整系数多项式。

18. (i) 必有$(q,a) = 1$, $q | a^{q-1} - 1$。因而$q | a^{(p,q-1)} - 1$。若$(p, q-1) = 1$, 则$q | a - 1$; 若$(p, q-1) = p$, 则$q \equiv 1 \pmod{2p}$;

(ii) $q | a^{2p} - 1$。同(i)的论证,并注意$q \nmid a - 1$;

(iii) 设 s 是给定的正整数,取 $a = 2^{p^{s-1}}$。设 q 是$(a^p - 1)/(a-1)$的素除数。先证$a \not\equiv 1 \pmod q$。用反证法。设δ是最小正整数使得 $2^\delta \equiv 1 \pmod q$。证明 $\delta = p^s$。进而推出 $p^s | q - 1$。以上论证对 $p = 2$也成立。当 $p > 2$时, $q = 2kp^s + 1$; 当 $p = 2$时, $q = 2^s k + 1$。由 s 的任意性就推出所要结论。

19. 显见,只要证 $p^s | \phi(b^{p^s} - 1)$, p 为素数。取$a = b^{p^{s-1}}$,所要证的结论可从 $p^s | \phi((a^p - 1)/(a-1))$推出。当 $b = 2$ 时,第18题(iii)已证$(a^p - 1)/(a-1)$的素因数 $q = 2kp^s + 1$, 当 $p > 2$; $= 2^s k + 1$, 当 $p = 2$。这就证明了所要结论。当 $b > 2$时可类似证明,但要注意可能出现的 $q | a - 1$的情形。这时有 $q = p | b - 1$, 要直接证 $p^s | \phi(b^{p^s} - 1)$, 而这只要证明 $p^{s+1} | b^{p^s} - 1$。

20. 必有正整数 d_0, 使$9a | 10^{d_0} - 1 = 99\cdots9 = 9 \cdot (11\cdots1)$, d_0位1。所以, a 整除$11\cdots1$, 这里有 $d_0 k$ 位 1, $k = 1, 2, 3, \cdots$。

21. 第一部分利用上题。末位数不是0,5的不能被5整除,末位数为5的不能被2整除。

22. 证明$a^{l\phi(r)-1}$都属于这算术数列, $l = 0, 1, 2, \cdots$。

23. $d_0 = 2^{l-2}$。

24. 必有 $a \equiv b \pmod p$。

26. 式中的乘积 $= \begin{cases} 1, & 当(l, n) = 1; \\ 0, & 当(l, n) > 1. \end{cases}$

习 题 四

1．利用定理 1．

2．(i) 用反证法，并注意$p>5$时必有$(p-1)|(p-2)!$。若$(p-1)!+1=p^k$，则必有$(p-1)|k$。矛盾；(ii) 同理论证。

3．分别对$n,n+2$利用第 1 题的(i)，(iii)(取$k=3$)。

4．利用定理 1，Fermat 小定理。

5．$p\nmid a$时，利用定理 1 及 Fermat 小定理。

6．(i) 用反证法。考虑$ij\equiv-1(\bmod p),1\leqslant i,j\leqslant p-1$。若有$i=j=i_0$使$i_0^2\equiv-1(\bmod p)$，这种$i_0(1\leqslant i_0\leqslant p-1)$恰有两个。由此推出$(p-1)!\equiv 1(\bmod p)$，和定理 1 矛盾；

(ii) 见例2；

(iii) 设$p_1,\cdots,p_r$均为$4m+1$形式的素数．考虑$(2p_1\cdots p_r)^2+1$的素因数。

7．用反证法。利用定理 2，定理 3．

8．由上题推出。

9．不一定。如对模 8 可取：$r_1=-3,r_2=-1,r_3=1,r_4=3$，$r_1'=3,r_2'=-3,r_3'=1,r_4'=-1$或$r_1'=1,r_2'=-1,r_3'=3,r_4'=-3$。对模15可取：$r_i$依次为$-7,-4,-2,-1,1,2,4,7$，$r_i'$依次为$2,-2,4,-4,-1,1,7,-7$。

10．一定有$(r_i,m)=1\Longleftrightarrow(r_i',m)=1$。所以不和$m$既约的$r_i$一定是同不和$m$既约的$r_i'$相乘。对给定的$d>1$，在一个完全剩余系中同$m$的最大公约数为$d$的数的个数是一定的。由这两点就可推出矛盾。

第 四 章

习 题 一

1．(i) $x\equiv 1,5(\bmod 7)$；(ii) $x\equiv-1(\bmod 11)$；

(iii) $x\equiv 1,3,15,17 \pmod{28}$; (iv) $x\equiv 3,5,17,19 \pmod{28}$;

(v) $x\equiv -5,-3,9,11 \pmod{28}$;

(vi) 无解。$141=3\cdot 47$。$4x^2+21x-32\equiv x^2+1\equiv 0 \pmod 3$ 无解；(vii) 利用 $x^5\equiv x \pmod 5$ 化简，原方程变为：$2x^3-2x^2-2\equiv 0 \pmod 5$，无解；(viii) 利用 $x^7\equiv x \pmod 7$ 化简，变为 $x^6+3x^4+x-1\equiv 0 \pmod 7$，$x=0$ 不是解，当 $x\not\equiv 0 \pmod 7$ 时，方程变为 $3x^3+1\equiv 0 \pmod 7$，无解。

2．原方程等价于 $4a(ax^2+bx+c)\equiv(2ax+b)^2+4ac-b^2\equiv 0 \pmod m$。

3．$p^\alpha \mid a^2$ 的充要条件是 $p^{[(\alpha+1)/2]} \mid a$。

6．$a\equiv 0,\pm 1 \pmod 9$。

7．以 $x=2k,2k+1$ 代入。$1\equiv 2^{2k}\equiv(2k)^2\equiv k^2 \pmod 3$，$k\equiv \pm 1 \pmod 3$，得正整数 $x\equiv \pm 2 \pmod 6$ 是解；$2\equiv 2^{2k+1}\equiv(2k+1)^2\equiv k^2+k+1 \pmod 3$，无解。

8．$\{0 \bmod 5, \pm 1 \bmod 5\}$，$\{0 \bmod 5, \pm 2 \bmod 5\}$，
$\{\pm 1 \bmod 5, 0 \bmod 5\}$，$\{\pm 2 \bmod 5, 0 \bmod 5\}$。

9．因对任意整数 a，$3\nmid a$，$a^3\equiv \pm 1 \pmod 9$。

10．利用第三章习题三第 15 题 (ii) 的结果：$x^m\equiv x^{m-\phi(m)} \pmod m$，就可把同余方程的次数化为小于 m。在合数模情形，则可利用(iii)的结果。

11．当 $f(x)=ax-b$ 时，令 $d=m/(a,m)$。我们有

$$\sum_{l=0}^{m-1}\sum_{x=0}^{m-1} e^{2\pi i l(ax-b)/m}=\sum_{l=0}^{m-1} e^{-2\pi i l b/m}\sum_{x=0}^{m-1} e^{2\pi i l a x/m}$$

$$=m\sum_{\substack{l=0\\ m\mid la}}^{m-1} e^{-2\pi i l b/m}=m\sum_{k=0}^{m/d-1} e^{-2\pi i b k d/m}$$

$$=\begin{cases} m(a,m), & \text{当}(a,m)=m/d\mid b,\\ 0, & \text{当}(a,m)=m/d\nmid b.\end{cases}$$

12．方法同上题。

习 题 二

1. (i) $x\equiv 3 \pmod 7$; (ii) $x\equiv 3,8,13 \pmod{15}$;

(iii) $x\equiv 9 \pmod{31}$; (iv) $(20,30)=10\nmid 4$, 无解;

(v) $x\equiv 7 \pmod{21}$; (vi) $x\equiv 62 \pmod{105}$;

(vii) $1001=7\cdot 11\cdot 13$. $x\equiv -189 \pmod{1001}$;

(viii) $x\equiv -1 \pmod{1597}$; (ix) $x\equiv -4,31,66 \pmod{105}$;

(x) $x\equiv -163 \pmod{999}$.

2. (i) $m=2l-1$. $x\equiv l^k b \pmod m$,然后求$l^k b$对模 $m=2l-1$的剩余; (ii) $m=3l\pm 1$, $x\equiv(\pm 1)^k l^k b \pmod m$, 然后求$l^k b$对模$m=3l\pm 1$的剩余.

3. (i) 以第1题(vi)为例. $2^6 x\equiv 83 \pmod{105}$. $x\equiv 52^6\cdot 83\equiv 1+52^6\cdot 19\equiv 1+13\cdot 13\cdot 19\equiv 1+64\cdot 19\equiv 62 \pmod{105}$;

(ii) $x\equiv 179\cdot 168^8\equiv 179\cdot 21\cdot 21\equiv 179\cdot 104\equiv 81 \pmod{337}$;

(iii) $243x\equiv 112 \pmod{551}$, $x\equiv 112\cdot 184^5\equiv 200 \pmod{551}$, $x\equiv 200+551\cdot t \pmod{2755}$, $t=0,1,2,3,4$;

(iv) $2^4\cdot 3^4 x\equiv 1105 \pmod{2413}$, $x\equiv 1105\cdot 402^4\equiv 1105\cdot 67\cdot 67\equiv -783 \pmod{2413}$,这里用$2413=6\cdot 402+1$

4. $m=[m/a]a+a_1$, $1\leqslant a_1<a$. $ax\equiv b \pmod m$ 的解一定是$a[m/a]x\equiv b[m/a] \pmod m$的解, 即是 $a_1 x\equiv -b[m/a] \pmod m$的解. 反过来不一定对. 要$([m/a],m)=1$时反过来才一定成立.

5. (i) $m=23$, $a=6$. $[23/6]=3$, $(3,23)=1$. 所以原方程等价于$5x\equiv -21\equiv 2 \pmod{23}$. $[23/5]=4$, $(4,23)=1$, $3x\equiv -8 \pmod{23}$. $[23/3]=7$, $(7,23)=1$, $2x\equiv 10 \pmod{23}$, $x\equiv 5 \pmod{23}$;

(ii) $[12/5]=2$, $(2,12)=2$, 所以不要用这方法.

7. (i) $3x\equiv 1 \pmod{5^3}$, $3\cdot 2\equiv 1 \pmod 5$, $1-(1-3\cdot 2)^3=126$, 所以$x=42$是原同余方程的解; (ii) $5x\equiv 1 \pmod{3^5}$. $5\cdot(-1)\equiv 1 \pmod 3$. $1-(1-5\cdot(-1))^5=-7775$. $x=-1555$ 是

解。

8. $ay+b\equiv x \pmod m$确定了 $g(y)\equiv 0 \pmod m$的解 $y \bmod m$ 与 $f(x)\equiv 0 \pmod m$的解 $x \bmod m$ 之间的一一对应。

9. 若 x_0 是 $ax\equiv b \pmod m$的一解。取$y_0=(b-ax_0)/m$。$x=x_0+mt/(a,m)$，$y=y_0-mt/(a,m)$，$t=0,\pm1,\pm2,\cdots$，就给出了不定方程的解。

习 题 三

1. (i) $x=1+4y$，$4y\equiv 1 \pmod 3$，$4y\equiv 2 \pmod 5$。进而，$y\equiv 1 \pmod 3$。$y\equiv -2 \pmod 5$。$y=1+3z$，$3z\equiv -3 \pmod 5$，$z\equiv -1 \pmod 5$。$y\equiv -2 \pmod{15}$，$x\equiv -7 \pmod{60}$；

(ii) $x=4+11y$，$11y\equiv -1 \pmod{17}$，$y\equiv 3 \pmod{17}$，$x\equiv 37 \pmod{187}$；

(iii) $m_1=5, m_2=6, m_3=7, m_4=11$，$M_1=6\cdot7\cdot11\equiv 2 \pmod 5$，$3M_1\equiv 1 \pmod{m_1}$。$M_2=5\cdot7\cdot11\equiv 1 \pmod 6$，$1\cdot M_2\equiv 1 \pmod{m_2}$。$M_3=5\cdot6\cdot11\equiv 1 \pmod 7$，$1\cdot M_3\equiv 1 \pmod{m_3}$。$M_4=5\cdot6\cdot7\equiv 1 \pmod{11}$，$1\cdot M_4\equiv 1 \pmod{11}$。所以 $x\equiv 3\cdot6\cdot7\cdot11\cdot2+5\cdot7\cdot11\cdot1+5\cdot6\cdot11\cdot3 \pmod{5\cdot6\cdot7\cdot11}$；

(iv) $x=4+11y$，$55y\equiv 0 \pmod{13}$，$x\equiv 4 \pmod{143}$；

(v) $x=-3+5y$，$15y\equiv 2 \pmod{17}$，$y\equiv -1 \pmod{17}$，$x\equiv -8 \pmod{85}$。$x\equiv -8, 77 \pmod{170}$；

(vi) $x\equiv 27 \pmod{60}$；

(vii) 无解。第二，第三两个方程矛盾。

2. (i) $x\equiv -1 \pmod 4$，$2x\equiv -1 \pmod 5$，$2x\equiv 1 \pmod 7$，得到解为 $x\equiv 67 \pmod{140}$；

(ii) $x\equiv 1 \pmod 4$，$2x\equiv -1 \pmod 5$，$3x\equiv 5 \pmod 7$，$2x\equiv 3 \pmod{11}$。得到解 $x\equiv 557 \pmod{1540}$。

3. $x\equiv 1 \pmod 3$，$x\equiv 2 \pmod 4$，$x\equiv 3 \pmod 5$。解为 $x\equiv -2 \pmod{60}$。

4. 使$7x+1\equiv 0 \pmod{10}$成立的最小正整数，及使$7x\equiv 0 \pmod{10}$成立的最小正整数中，小的一个即为要求的周数，即7周后可在星期天休息。

5. 设$p_1,\cdots,p_k$是两两不同的正整数。考虑同余方程组：$x\equiv -j+1 \pmod{p_j^3}$，$j=1,\cdots,k$。若$x_0$是解，则$x_0,x_0+1,\cdots,x_0+k-1$就满足要求。

6. 同上题方法，以a_j代p_j^3。

7. 设能整除c但不能整除b的所有素因数是$p_1,\cdots,p_r$。满足同余方程组$bx+a\equiv 1 \pmod{p_j}$，$1\leqslant j\leqslant r$的x即满足要求。

8. 不两两既约时不成立。

11. (i) 设$m_j=p_1^{a_{1j}}\cdots p_r^{a_{rj}}$，$1\leqslant j\leqslant k$，$m=p_1^{a_1}\cdots p_r^{a_r}$，$a_i=\max\limits_{1\leqslant j\leqslant k}(a_{ij})$。先在每个$m_j$中保留和$m$中同方幂的那些素数幂，其它删去，得到$m_j''$，若$p_i^{a_i}$出现在两个或两个以上的$m_j''$中，则只保留最小指标$j_0$的$m_{j_0}''$中的这一方幂，其它的均删去。这样得到$m_j'(1\leqslant j\leqslant k)$，这些$m_j'$就满足要求；

(ii) $x\equiv a_j \pmod{m_j}(1\leqslant j\leqslant k)$的解一定是$x\equiv a_j \pmod{m_j'}(1\leqslant j\leqslant k)$的解，且均对模$m$有唯一解，所以解相同。

12. (i) $x\equiv -6 \pmod{13}$，$y\equiv -4 \pmod{13}$； (ii) $x\equiv y\equiv 2 \pmod{5}$； (iii) 无解； (iv) $x\equiv y-2 \pmod{5}$； (v) $x\equiv 2y-1 \pmod{7}$；(vi) 无解。

习 题 四

1. (i) $x\equiv -17,-12,-7,1,6,11 \pmod{45}$；(ii) $x\equiv 10 \pmod{33}$；(iii) $x\equiv -65\cdot x_1+66\cdot x_2 \pmod{143}$，$x_1=1,3,5$，$x_2=1,3,5$。

2. (i) $x\equiv -10 \pmod{3^3}$；(ii) $x\equiv -12 \pmod{3^3}$； (iii) $x\equiv 11 \pmod{3^4}$；(iv) 无解；(v) $x\equiv -56,-2+25\cdot j,8+25j \pmod{5^3}$，$j=0,\pm 1,\pm 2$； (vi) $x\equiv 4 \pmod{5^3}$； (vii) 无解； (viii) $x\equiv 23 \pmod{7^3}$； (ix) $x\equiv 2+9j \pmod{3^3}$，$j=0,\pm 1$； (x) 无解；

(xi) $x\equiv\pm578 \pmod{11^3}$； (xii) $x\equiv\pm(2590+4\cdot19^3)\equiv\pm30026 \pmod{19^4}$。

3．原方程等价于$(x^2+x+1)^2\equiv0 \pmod{7^6}$，进而等价于$x^2+x+1\equiv0 \pmod{7^3}$。$x\equiv-19,18 \pmod{7^3}$。(这是全部解，不是解数)。

7．由例4，例5推出。

8．化为$(x-1)(x+1)\equiv0 \pmod{p^l}$的同余方程组，再用例4，例5。

10．先证明对素数p，$x^2\equiv x \pmod{p^k}$的解数一定为2，k为任意正整数。

12．利用推论4．

14．设$f(x)=a_nx^n+\cdots+a_1x+a_0$。$n\geqslant1, a_n\neq0$。当$a_0=0$时结论成立。当$a_0\neq0$时，$f(a_0x)=a_0(b_nx^n+\cdots+b_1x+1)=a_0g(x)$，$b_n\neq0$。若$g(x)\equiv0 \pmod p$只对有限个$p=p_1,p_2,\cdots,p_r$可解，则$p_j\nmid g(p_1\cdots p_rx)$，$j=1,\cdots,r$。所以$g(p_1\cdots p_rx)$必有不同于$p_1,\cdots,p_r$的素因数，矛盾。由此推出所要结论。

15．由上题及孙子定理知，必有x_0使$f(x_0)$有s个不同的素因数，设为$p_1,\cdots,p_s$．这就证明了结论对$r=1$成立。令$P=p_1\cdots p_s$；对任意t，$f(x_0+Pt)$也一定至少有s个素因数。再考虑t的多项式$F(t)=f(x_0+Pt+1)$，由结论对$r=1$成立知，必有$t=t_0$使$F(t_0)=f(x_0+Pt_0+1)$有s个不同的素因数。这就证明了结论当$r=2$成立。进而利用归纳法，用同样的论证就可证明所要结论。

习　题　五

1．$p=13$。二次剩余：1,3,4,9,10,12；$p=23$。二次剩余：1,2,3,4,6,8,9,12,13,16,18；$p=37$。二次剩余：1,3,4,7,9,10,11,12,16,21,25,26,27,28,30,33,34,36；$p=41$。二次剩余：1,2,4,5,8,9,10,16,18,20,21,23,25,31,32,33,36,37,39,40。

2．以 2 为二次剩余的模 p 是：7，17，23，31，41，47，71，73，79，87，97。

3．(i) $(-8)^{26}\equiv 11^{13}\equiv 11\cdot 15^6\equiv 11\cdot 13^3\equiv -16\cdot 10\equiv -1 \pmod{53}$，$-8$不是模53的二次剩余；(ii) $8^{33}\equiv 8\cdot(3)^{16}\equiv 8\cdot 14^4\equiv 8\cdot 5^2\equiv -1 \pmod{67}$。8不是模67的二次剩余。

4．(i) 2；(ii) 0；(iii) 0；(iv) 0；(v) $221=13\cdot 17$，4个解；(vi) $427=7\cdot 61$，无解；(vii) $209=11\cdot 19$，4 个解；(viii) $391=17\cdot 23$。4 个解。(ix) $45=3^2\cdot 5$。4 个解。(x) $539=7^2\cdot 11$。4 个解。

5．若 $u^2+av^2\equiv 0 \pmod p$ 成立，则必有 $p\nmid uv$。因而有 $vv'\equiv 1 \pmod p$，$(v'u)^2\equiv -a \pmod p$。

6．由条件(i)和(ii)知模 p 的全部二次剩余均属于S_1。由条件(i)和(iii)知S_2中的元素个数不会少于 S_1 中的元素个数。由此及定理 1 就推出所要结论。

7．(i)，(ii)利用 Wilson 定理；(iii) 即求$1^2+2^2+\cdots+((p-1)/2)^2$ 对模 p 的剩余，用平方和公式；(iv)由(iii)来求。

9．(i) 由 Euler 定理推出必要性。但不充分．例如，$m=15$ 时二次剩余仅有 1，4．但 $2^4\equiv 1 \pmod{15}$，2 不是二次剩余；

(ii) $x^2\equiv a \pmod m$ 等价于$(x^{-1})^2\equiv b \pmod m$，$x^{-1}$ 表 x 对模 m 的逆；

(iii) 按 $ab\equiv 1 \pmod p$ 来把所有二次剩余两两分组，并注意 -1 是二次剩余当且仅当 $p\equiv 1 \pmod 4$；

(iv) 不成立；

(v) 不一定．例如，对模12，二次剩余只有 1，而5，7，11 均为二次非剩余，它们中任意两个不同的数之积均仍为二次非剩余；

(vi) 设 $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$。$\{a\}$，$\{a_0\}$，$\{a_1\}$，…，$\{a_r\}$分别表模 m，模$p_0^{\alpha_0}(p_0=2)$，模$p_1^{\alpha_1}$，…，模$p_r^{\alpha_r}$的既约剩余系，由孙子定理知，a 是模 m 的二次剩余的充要条件是，$a_0,a_1,\cdots,a_r$ 分别是模$p_0^{\alpha_0}$，$p_1^{\alpha_1}$，…，$p_r^{\alpha_r}$ 的二次剩余，这里$a\equiv a_j \pmod{p_j^{\alpha_j}}$，$0\leqslant j\leqslant r$。再对每

个 j,讨论 $x^2\equiv a_j(\bmod p_j^{\alpha_j})$的解数，及使其有解的 a_j 的个数(利用 §4的方法)。

10. 这时 j 和 $p-j$ 必同为二次剩余或二次非剩余，$1\leqslant j\leqslant(p-1)/2$。并利用定理 1。

11. 设 $j^2=pq_j+r_j,1\leqslant r_j<p,1\leqslant j\leqslant(p-1)/2$。由此及 $q_j=[j^2/p]$即得：$S=\sum r_j=\sum j^2-p\sum[j^2/p]$。再利用第10题(ii)。

13. 考虑集合$\{ax+y:\ 0\leqslant x\leqslant[\sqrt{m}],0\leqslant y\leqslant[\sqrt{m}]\}$，其元素个数$=([\sqrt{m}]+1)^2>m$。用鸽巢原理及$(a,m)=1$。

14. 当m不是平方数时由上题推出；当m是平方数时，考虑集合$\{ax+y:\ 0\leqslant x\leqslant\sqrt{m},0\leqslant y\leqslant\sqrt{m}-1\}$，其元素个数$=(\sqrt{m}+1)\sqrt{m}>m$。用鸽巢原理及$(a,m)=1$。

15. 同第13题的证法。

16. 利用提示，由第14题知所考虑的同余方程必有解$0<|x_0|,|y_0|<\sqrt{p}$，不妨设$x_0>0$。若x_0不是二次非剩余，则$\pm y_0$一定都是二次非剩余(因$p\equiv1(\bmod 4)$)。所以，必有一正数c，$0<c<\sqrt{p}$，是二次非剩余。由于$p\equiv1(\bmod 8)$，2是模p的二次剩余，及c必有一素因数是模p的二次非剩余，就推出所要结论。

习 题 六

1. $-1,-1,1,1,1,1,-1,1,-1,1$。

2. (i) $\left(\frac{7}{227}\right)=1$，有解；(ii) $511=7\cdot73$，$\left(\frac{11}{73}\right)=-1$，无解；(iii) $91=7\cdot13$，$\left(\frac{11}{7}\right)=\left(\frac{-6}{7}\right)=1$，$\left(\frac{11}{13}\right)=\left(\frac{-6}{13}\right)=-1$，有解；(iv) $6193=11\cdot563$，$\left(\frac{5}{11}\right)=1\neq\left(\frac{-14}{11}\right)=-1$，无解。

3. (i) $p\equiv1(\bmod 6)$；(ii) $p\equiv1(\bmod 12)$；(iii) $p\equiv5(\bmod 12)$；(iv) $p\equiv-1(\bmod 12)$；(v) $p\equiv-5(\bmod 12)$；(vi) $(100)^2-3$的素因数$p\equiv\pm1(\bmod 12)$。$100^2-3=13\cdot769$；150^2+3的素因数

$p\equiv 1 \pmod 6$)，及 $p=3$，$150^2+3=3\cdot 13\cdot 577$。

4．$p\equiv \pm 7 \pmod{24}$。

5．(i) $p\equiv \pm 1 \pmod 5$；(ii) $p\equiv 1,3,7,9 \pmod{20}$；(iii) $121^2-5=14636$ 是 $2^2\cdot 3659$，$121^2+5=14646=2\cdot 3\cdot 2441$；$82^2+5\cdot 11^2=7329=3\cdot 7\cdot 349$；$82^2-5\cdot 11^2=6119=29\cdot 211$；$273^2+5\cdot 11^2=2\cdot 37567$，$273^2-5\cdot 11^2=2^2\cdot 18481$；(iv) 由(i)和(ii)知不可解。

6．(i) $p\equiv 1,3 \pmod 8$；(ii) $p\equiv \pm 1,\pm 3,\pm 9,\pm 13 \pmod{40}$。

7．(i) $p=2$，$p=13$，及 $p\equiv \pm 1,\pm 3,\pm 4 \pmod{13}$；(ii) $n^4-n^2+1=(n^2-1)^2+n^2=(n^2+1)^2-3n^2$。

8．(i) 证 $8k-1$ 形式的素数有无穷多个，利用 $(p_1\cdots p_r)^2-2$；证 $8k+3$ 形式的素数有无穷多个，利用 $(p_1\cdots p_r)^2+2$；证 $8k-3$ 形式的素数有无穷多个，利用 $4(p_1\cdots p_r)^2+1$；

(ii) 依次利用 $3(p_1\cdots p_r)^2+1$，$3(p_1\cdots p_r)^2+1$（和 $3k+1$ 形式同），$4(p_1\cdots p_r)^2+3$，$(p_1\cdots p_r)^4-(p_1\cdots p_r)^2+1$（利用第 7 题 (ii)）；

(iii) 利用第 5 题(i)，及考虑 $5(n!)^2-1$，证明 $10k-1$ 形式的素数有无穷多个。

9． d 是素数时成立

10．(i) $p\mid ab$ 结论成立；$p\nmid ab$，则 $\left(\frac{a}{p}\right)$，$\left(\frac{b}{p}\right)$，$\left(\frac{ab}{p}\right)$ 必有一为1；

(ii) 原多项式 $=(x^2-2)(x^2-3)(x^2-6)$。

11．$x^4+4=((x-1)^2+1)((x+1)^2+1)$。

12．(i) $x^8-16=(x^4+4)(x^2-2)(x^2+2)$，并利用上题；(ii) $l\geqslant 3$ 时，$x^8-16\mid x^{2^l}-2^{2^{l-1}}$。

13．(i) $(a^{(n+1)/2})^2\equiv a \pmod p$；(ii) 由(i)及定理 3 推出。

14．(i) $2^{22}-1=(2^{11}-1)(2^{11}+1)\equiv 0 \pmod{23}$，$23\equiv -1 \pmod 8$，所以 $2^{11}+1\not\equiv 0 \pmod{23}$，另两个同样证明；(ii) $(2^p-1)(2^p+1)=2^{2p}-1\equiv 0 \pmod{2p+1}$，及 $2p+1\equiv 7 \pmod 8$，利用第6题(i)。

15．必要性。设 q 是素数。若结论不成立，则 $\left(\frac{3}{q}\right)=1$，进而

推出 $q\equiv\pm1 \pmod{12}$，矛盾。充分性。设使 $3^h\equiv1 \pmod q$ 成立的最小 h 为 h_0。$h_0 | q-1=2^{2^n}$，由此及 $3^{2^{2^n-1}}\not\equiv1 \pmod q$ 得 $h_0=q-1$，所以 q 是素数。

16. (i) 利用 Euler 判别法；

(ii) 利用 Euler 判别法及 $\left(\frac{-2}{p}\right)=-1$。解的形式可分开来写为：当 $a^{2m+1}\equiv1 \pmod p$ 时，$x_0=\pm a^{m+1}$，当 $a^{2m+1}\equiv-1 \pmod p$ 时，$x_0=\pm2^{2m+1}a^{m+1}$；

(iii) 同(ii)的方法，b的作用相当于(ii)中的2。设$p=2^l n+1$，$l\geqslant3$，$2\nmid n$。我们有$a^{2^{l-2}n}\equiv\pm1 \pmod p$，及$b^{2^{l-1}n}\equiv-1 \pmod p$。进而推出必有非负整数 s_1 使 $a^{2^{l-2}n}\cdot b^{s_1 2^{l-1}}\equiv1 \pmod p$。因而有 $a^{2^{l-3}n}b^{s_1 2^{l-2}}\equiv\pm1 \pmod p$。由此再利用$b^{2^{l-1}n}\equiv-1 \pmod p$，重复前面的论证，可推出：必有非负整数 s_2，使得$a^{2^{l-3}n}b^{s_2 2^{l-2}}\equiv1 \pmod p$，及$a^{2^{l-4}n}b^{s_2 2^{l-3}}\equiv\pm1 \pmod p$。这样，最后可得：存在非负整数 s_k 使$a^n b^{2s_k}\equiv1 \pmod p$。所以，解$x_0=\pm a^{(n+1)/2}\cdot b^{s_k}$。

17. (i)

p \ d n	2	3	5	7	13
11	3	2	2	3	
17	4	3	3	3	4
19	5	3	4	4	3
29	7	5	6	6	6

(ii) 仿照例 3 中直接用引理 2 证$\left(\frac{3}{p}\right)$的方法。

18.19.20. 这三题的证明可仿照引理 2。

22. 仿照定理 3 与例 3 中的论证。

23.24.25. 仿照定理 4 的论证。

27．当 $p\equiv3(\mathrm{mod}\ 8)$时，$\left(\frac{2}{p}\right)=-1.2,4,6,\cdots,p-1$中为二次剩余的整数个数就是 $1,2,\cdots,(p-1)/2$ 中的二次非剩余个数，由此及习题五第12题(iii)推出$R^{(2)}=N_1$．当 $p\equiv7(\mathrm{mod}\ 8)$时，$\left(\frac{2}{p}\right)=1$．$2,4,6,\cdots,p-1$ 中的二次剩余的个数即 $1,2,\cdots,(p-1)/2$ 中的二次剩余个数，由此及习题五第12题(iii)得 $R^{(2)}=(p-1)/2-N_1$（注意：当 $p\equiv1(\mathrm{mod}\ 4)$时，由同样的论证及习题五第12题 (iii)，(iv)可知，$R^{(2)}=(p-1)/4$．）．

28．先证(iii)．设 N_1 同第 27 题，$N_1+R_1=(p-1)/2$．易证：$((p-1)/2)!\equiv(-1)^{N_1}(((p-1)/2)!)^2(\mathrm{mod}\ p)$．再利用第三章习题四第 4 题(ii)即得(iii)．由(iii) 及 $2\cdot4\cdots(p-1)=2^{(p-1)/2}((p-1)/2)!$，就推出(i)，(ii)．

29．因为$\left(\frac{2}{q}\right)=\left(\frac{2-q}{q}\right)$．

30．(i) 用反证法．若$b^2+2\mid4a^2+1$，则$2\nmid b$，$b^2+2\equiv3(\mathrm{mod}\ 4)$．所以 b^2+2 一定有素因数 $p\equiv3(\mathrm{mod}\ 4)$，但 $p\mid4a^2+1$ 必有 $p\equiv1(\mathrm{mod}\ 4)$，矛盾；

(ii) 证法同(i)；

(iii) 若 $2b^2+3\mid a^2-2$，由于 $2b^2+3\equiv\pm3(\mathrm{mod}\ 8)$，所以必有素数 $p\equiv3(\mathrm{mod}\ 8)$或$-3(\mathrm{mod}\ 8)$，$p\mid2b^2+3$．但 $p\mid a^2-2$，必有 $p\equiv\pm1(\mathrm{mod}\ 8)$，矛盾；

(iv) 若$3b^2+4\mid a^2+2$，则$2\nmid b$，$3b^2+4\equiv7(\mathrm{mod} 8)$，所以 $3b^2+4$ 必有素因数 $p\equiv5$ 或 $7(\mathrm{mod}\ 8)$．但 $p\mid a^2+2$，必有$p\equiv1,3(\mathrm{mod}\ 8)$（见第 6 题），矛盾．

32．x 和 $ax+b$ 同时遍历模 p 的完全剩余

33．以 $x^{-1}=y$ 表示 x 对模 p 的逆，x，y 同时遍历模 p 的既约剩余系．

$$\sum_{x=1}^{p}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p}\left(\frac{(ax)^2+a(ax)}{p}\right)$$

$$= \sum_{x=1}^{p-1}\left(\frac{x^2+x}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{y^2(x^2+x)}{p}\right)$$

$$= \sum_{x=1}^{p-1}\left(\frac{1+y}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{1+x}{p}\right) = -1.$$

34. $4af(x) = (2ax+b)^2 - \Delta$, $\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right) = \left(\frac{a}{p}\right)\sum_{x=1}^{p}\left(\frac{x^2-\Delta}{p}\right)$.

当 $p\mid\Delta$ 时，由此推出(ii)成立。当 $p\nmid\Delta$ 时，分 $\left(\frac{\Delta}{p}\right)=1$，$\left(\frac{\Delta}{p}\right)=-1$ 两种情形。当 $\left(\frac{\Delta}{p}\right)=1$ 时，设 $d^2\equiv\Delta\pmod p$。我们有

$$\sum_{x=1}^{p}\left(\frac{x^2-\Delta}{p}\right) = \sum_{x=1}^{p}\left(\frac{(x-d)(x+d)}{p}\right) = \sum_{x=1}^{p}\left(\frac{x(x+2d)}{p}\right) = -1, \tag{*}$$

最后一步用到了第33题。所以这时结论成立。但当 $\left(\frac{\Delta}{p}\right)=-1$ 时不能用这方法，要困难得多。下面的证法可统一讨论 $p\nmid\Delta$ 的情形。显见，我们需要知道有多少个 x $(1\leqslant x\leqslant p)$ 使得 $x^2-\Delta$ 是模 p 的二次剩余（包括 $p\mid x^2-\Delta$ 的情形），这就是要讨论同余方程 $x^2-\Delta\equiv y^2\pmod p$ 的解数 T。显见

$$T = \sum_{x=1}^{p}\left(1+\left(\frac{x^2-\Delta}{p}\right)\right) = p + \sum_{x=1}^{p}\left(\frac{x^2-\Delta}{p}\right).$$

但另一方面，T 可以这样来计算：以 t_u 表同余方程组 $y^2\equiv u\pmod p$，$x^2\equiv u+\Delta\pmod p$ 的解数，则 $t_u = \left(1+\left(\frac{u}{p}\right)\right)\left(1+\left(\frac{u+\Delta}{p}\right)\right)$，

$T = \sum_{u=1}^{p} t_u$。因而，

$$T = \sum_{u=1}^{p}\left\{1+\left(\frac{u}{p}\right)+\left(\frac{u+\Delta}{p}\right)+\left(\frac{u(u+\Delta)}{p}\right)\right\} = p-1,$$

这里用到了第32题，第33题。由 T 的这两个关系式推出这时式

(*)也成立，这就证明了所要的结论。

35. $x^4+1\equiv(x^2+1)^2 \pmod 2$，所以可设 $p\geqslant 3$. 若$\left(\frac{-1}{p}\right)=1$，则取$b$满足$b^2\equiv -1 \pmod p$，就有 $x^4+1\equiv(x^2-b)(x^2+b) \pmod p$. 若$\left(\frac{-1}{p}\right)=-1$，设 a,b,c,d 为待定整数，要求满足所说的关系式，及 $p\nmid abcd$. 这时 $p\equiv 3 \pmod 4$. 易证：当 $p\equiv 3 \pmod 8$时，可取a满足$a^2\equiv -2 \pmod p$，$c\equiv -a \pmod p$，$b=d=-1$；当$p\equiv 7 \pmod 8$时，可取 a 满足 $a^2\equiv 2 \pmod p$，$c\equiv -a \pmod p$，$b=d=1$.

习 题 七

1. (i) -1；(ii) 1；(iii) 1；(iv) -1.

2. 以 $4|a$ 为例. 设 $a=2^{\alpha}n$，$\alpha\geqslant 2$，$2\nmid n$. 利用互反律得

$$\left(\frac{a}{2a+b}\right)=\left(\frac{2^{\alpha}}{2a+b}\right)\left(\frac{b}{n}\right)(-1)^{(k-1)(b-1)/4},$$

$$\left(\frac{a}{b}\right)=\left(\frac{2^{\alpha}}{b}\right)\left(\frac{b}{n}\right)(-1)^{(k-1)(b-1)/4},$$

$2|\alpha$ 时由此推出结论成立；$2\nmid\alpha$时，利用式 (2) 直接验证$\left(\frac{2}{2a+b}\right)=\left(\frac{2}{b}\right)$，所以结论也成立。其它类似验证。

3. 同上题的证法。

4. 充分性显然。必要性用反证法。设 $a=b^2a_1$，$a_1\neq 1$ 且不是平方数，即 $a_1=\pm 2^{\alpha_0}p_1\cdots p_r$（$\alpha_0=0,1$；$p_i$ 为两两不同的奇素数）。设 d_r 是模 p_r 的二次非剩余。由提示知，必有素数 $p\equiv 1 \pmod 8$，$p\equiv 1 \pmod{p_i}$，$1\leqslant i\leqslant r-1$，及 $p\equiv d_r \pmod{p_r}$，进而推出$\left(\frac{a_1}{p}\right)=-1$，矛盾。

习　题　八

2．(i) $(x-1)(x+2)(x^2+2)+7(2x^5-x^4+x^3+x^2-2x+1)$；

(ii) $(x-1)(x^3+4x^2+4x+5)+7(x^4+2)=(x-1)^2(x^2-x+2)+7(x^3+x+1)$；

(iii) $(x-1)(x+1)(x^5-3x^4+2x^3+4x^2-3x-1)+13(x^6+x^4+x^3-x^2)=(x-1)^2(x+1)^2(x^3-3x^2+3x+1)+13(x^6+x^4+x^3-x^2)$。

4．(i)原同余方程的解和同余方程 $x^3+2x^2-x+3\equiv0 \pmod 5$ 相同，

$$x^5-x=(x^2-2x)(x^3+2x^2-x+3)+5(x^3-5x^2+5x);$$

(ii) $x\equiv0 \pmod{13}$ 不是它的根．$x^{12}-1=(x^6-4x^5+6x^4+6x^3+3x^2-2x+3)\cdot(x^6+4x^5+10x^4+10x^3-47x^2-318x-1075)+13(-164x^5+653x^4-560x^3+21x^2-92x+248)$。

5．(i) $x^5+x^2-3\equiv0 \pmod 7$；(ii) $x^4-2x^3-x+2\equiv0 \pmod 5$；

(iii) $x^6-3x^4+x^3+2x-1\equiv0 \pmod 7$；

(iv) $x^{10}+4x^9-x^8-x^6+x^4+x^3+2x-5\equiv0 \pmod{11}$。

6．(i) 模 7 的二次剩余是：1，2，4；三次剩余是：-1，1；四次剩余是：1，2，4；五次剩余是：1，2，3，4，5，6；(ii) 模 13 的二次剩余是：±1，±3，±4；三次剩余是：±1，±5；四次剩余是：1，3，-4；五次剩余是：±1，±2，±3，±4，±5，±6；(iii) 模17的二次剩余是：±1，±2，±4，±8；三次剩余是：±1，…，±8；四次剩余是：±1，±4；八次剩余是：±1；(iv) 模19的二次剩余是：1，-2，-3，4，5，6，7，-8，9；三次剩余是：±1，±7，±8；四次剩余是：1，-2，-3，4，5，6，7，-8，9；五次剩余是：±1，…，±9；六次剩余是：1，7，-8。

7．-1，3是模 7 的四次非剩余，-3仍是四次非剩余；±2是模19的三次非剩余，-4仍是三次非剩余。

9. $x^4\equiv -2 \pmod 7$无解。$2=(4,7-1)=2\cdot 4-(7-1)$，$r=2$，$s=1$。$x^2\equiv(-2)^2\equiv 4 \pmod 7$有解。

第 五 章

习 题 一

1.

a	-2	-1	1	2
$\delta_5(a)$	4	2	1	4

$\phi(5)=\lambda(5)=4$。原根：2，3。

a	-5	-4	-3	-2	-1	1	2	3	4	5
$\delta_{11}(a)$	10	10	10	5	2	1	10	5	5	5

$\phi(11)=\lambda(11)=10$。原根：2，6，7，8。

a	-5	-1	1	5
$\delta_{12}(a)$	2	2	1	2

$\phi(12)=4\neq\lambda(12)=2$。无原根。

a	-6	-5	-4	-3	-2	-2	1	2	3	4	5	6
$\delta_{13}(a)$	12	4	3	6	12	2	1	12	3	6	4	12

$\phi(13)=\lambda(13)=12$。原根：2，6，7，11。

a	-5	-3	-1	1	3	5
$\delta_{14}(a)$	3	3	2	1	6	6

$\phi(14)=\lambda(14)=6$。原根：3,5。

a	−7	−4	−2	−1	1	2	4	7
$\delta_{15}(a)$	4	2	4	2	1	4	2	4

$\phi(15)=8\neq\lambda(15)=4$。无原根。

a	−8	−7	−6	−5	−4	−3	−2	−1	1	2	3	4	5	6	7	8
$\delta_{17}(a)$	8	16	16	16	4	16	8	2	1	8	16	4	16	16	16	8

$\phi(17)=\lambda(17)=16$。原根：3,5,6,7,10,11,12,14。

a	−9	−8	−7	−6	−5	−4	−3	−2	−1	1	2	3	4	5	6	7	8	9
$\delta_{19}(a)$	18	3	6	18	18	18	9	9	2	1	18	18	9	9	9	3	6	9

$\phi(19)=\lambda(19)=18$。原根：2,3,10,13,14,15。

a	−9	−7	−3	−1	1	3	7	9
$\delta_{20}(a)$	2	4	4	2	1	4	4	2

$\phi(20)=8\neq\lambda(20)=4$。无原根。

a	−10	−8	−5	−4	−2	−1	1	2	4	5	8	10
$\delta_{21}(a)$	6	2	3	6	6	2	1	6	3	6	2	6

$\phi(21)=12\neq\lambda(21)=6$。无原根。

a	−11	−10	−9	−8	−7	−6	−5	−4	−3	−2	−1
$\delta_{15}(a)$	11	11	22	22	11	22	11	22	22	22	2

a	1	2	3	4	5	6	7	8	9	10	11
$\delta_{23}(a)$	1	11	11	11	22	11	22	11	11	22	22

$\phi(23)=\lambda(23)=22$。原根：5,7,10,11,14,15,17,19,20,21。

a	-17	-13	-11	-7	-5	-1	1	5	7	11	13	17
$\delta_{36}(a)$	2	6	3	6	6	2	1	6	6	6	3	2

$\phi(36)=12\neq\lambda(36)=6$。无原根。

a	-19	-17	-13	-11	-9	-7	-3	-1	1	3	7	9	11	13	17	19
$\delta_{40}(a)$	2	4	4	2	2	4	4	2	1	4	4	1	1	2	4	2

$\phi(40)=16\neq\lambda(40)=4$，无原根。

a	-31	-29	-26	-25	-24	-23	-22	-20	-19	-17	-16	-13
$\delta_{63}(a)$	6	6	3	6	6	6	6	3	6	3	6	6

a	-11	-10	-8	-5	-4	-2	-1	1	2	4	5	8	10	11
$\delta_{63}(a)$	6	6	2	3	6	6	2	1	6	3	6	2	6	6

a	13	16	17	19	20	22	23	24	25	26	29	31
$\delta_{63}(a)$	6	3	6	6	6	3	6	6	3	6	6	6

$\phi(63)=36\neq\lambda(63)=6$。无原根。

2．依次为5,6,20,4,12,11,30。

3. (i)

$\lambda(m)$	1	2	3	4	5	6	7	8	12
m	1,2	4,8,3 6,12,24	无	16,5,10 20,40,80	无	7,14 28,56	无	32,96 160,480	$2^{\alpha_0}3^{\alpha_1}7^{\alpha_2}13$, $\alpha_0\leqslant4,\alpha_1\leqslant2,\alpha_2\leqslant1$ $2^{\alpha_0}3^{\alpha_1}7$, $\alpha_0=4,\alpha_1\leqslant2$

(ii) 由 $\lambda(m)$的定义——式(7)推出；(iii) 由(ii)推出。

4. 直接验证 2 不是原根，3 是原根。

5. $a=11,27$时，$\delta_{37}(a)=6$；$a=7,37$时，$\delta_{43}(a)=6$。

6. 若 $(x_1x_2,m)=1$，$x_1^n\equiv x_2^n\pmod m$，$(x_1x_2^{-1})^n\equiv1\pmod m$。设 $x_1x_2^{-1}$ 对模 m 的指数为 δ，则 $\delta\mid(n,\phi(m))$，所以 $\delta=1$，即$x_1\equiv x_2\pmod m$。

7. 充分性显然。若 $a\not\equiv1\pmod p$，$a^2\equiv1\pmod p$，则必有 $a\equiv-1\pmod p$，即必要性成立。对合数模条件不是必要的。如$\delta_{12}(\pm5)=2$。

8. 由$\delta_p(a)=3$，可得$a\not\equiv\pm1\pmod p$，$a^2+a+1\equiv0\pmod p$。所以$1+a\not\equiv1\pmod p$，$(1+a)^2\equiv1+2a+a^2\equiv a\not\equiv1\pmod p$，$(1+a)^3\equiv-1\pmod p$。因而有 $\delta_p(1+a)=6$。

9. 由 $m-1=\delta_m(a)\mid\phi(m)$推出 $\phi(m)=m-1$，即证。

10. (i) 由 $p\nmid a^{h/2}-1$，$p\mid a^h-1=(a^{h/2}-1)(a^{h/2}+1)$ 即得；

(ii) 由(i)得$(-a)^{h/2}\equiv a^{h/2}\equiv-1\pmod p$。设$h'=\delta_p(-a)$。我们有 $h/2=\delta_p(a^2)=\delta_p((-a)^2)=h'/(h',2)$，由此及 $h'\neq h/2$即得 $h'=h$；

(iii) 这时$(-a)^{h/2}\equiv-a^{h/2}\equiv1\pmod p$。由此及(ii)的论证即得 $h'=h/2$。

11. 由第10题(ii)推出。

12. 必要性由第10题(iii)推出。若 $\delta_p(-g)=(p-1)/2$，则 $g^{(p-1)/2}\equiv-1\pmod p$。由此及 $\delta_p(g)/(\delta_p(g),2)=\delta_p(g^2)=$

$\delta_p((-g)^2)=\delta_p(-g)/(\delta_p(-g),2)=(p-1)/2$就推出$g$是原根。

13. $a=\pm 5^l, l=2^{\alpha-2-i}t, 2\nmid t$。

14. 必要性。当$a\equiv\pm 1 \pmod 8$时，$a^{2^{\alpha-3}}\equiv 1 \pmod{2^\alpha}$。充分性仿照第三章§3例2证明。

15. (i) $F_n \mid 2^{2^{n+1}}-1$，所以$\delta_{F_n}(2)\mid 2^{n+1}$。由此及$F_n\nmid 2^{2^l}-1, l\leqslant n$就推出$\delta_{F_n}(2)=2^{n+1}$；

(ii) $\delta_p(2)\mid\delta_{F_n}(2)=2^{n+1}$。设$\delta_p(2)=2^d, d\leqslant n+1$即$p\mid 2^{2^d}-1, p\nmid 2^{2^{d-1}}-1$。若$d\leqslant n$，则$p\mid(2^{2^{d-1}}-1)(2^{2^{d-1}}+1)$，因而$p\mid 2^{2^{d-1}}+1$，这和Fermat数两两既约(见第一章§4例1(v))矛盾；

(iii) 由(ii)及$\delta_p(2)\mid p-1$推出；

(iv) 当$n>1$时，$2^{n+1}<2^{2^n}$；

(v) 设a是二次非剩余，若不是原根，设其指数$\delta=2^k, k<2^n$。因而$a^{(F_n-1)/2}\equiv 1 \pmod{F_n}$，$a$为二次剩余，矛盾；

(vi) $\left(\frac{\pm 3}{F_n}\right)=\left(\frac{3}{F_n}\right)=\left(\frac{F_n}{3}\right)=\left(\frac{2}{3}\right)=-1$，$\left(\frac{\pm 7}{F_n}\right)=\left(\frac{7}{F_n}\right)=\left(\frac{F_n}{7}\right)$，由此及$F_{n+2}\equiv F_n \pmod 7$推出$\left(\frac{F_n}{7}\right)=\left(\frac{3}{7}\right)=-1$，当$2\nmid n$；$\left(\frac{F_n}{7}\right)=\left(\frac{5}{7}\right)=-1$，当$2\nmid n$。所以由(v)推出结论成立。

16. (i) $2^{2q}\equiv 1 \pmod p$。只要证$2^2\not\equiv 1 \pmod p$及$2^q\not\equiv 1 \pmod p$，由于$p>3$第一式成立。若$2^q\equiv 1 \pmod p$，则$2^{q+1}\equiv 2 \pmod p$，所以2是模p的二次剩余，$p\equiv\pm 1 \pmod 8$，但现在$p\equiv 3 \pmod 8$，矛盾；

(ii) 同(i)的论证。若不然，-2必为模p的二次剩余，所以$p\equiv 1,3 \pmod 8$(第四章习题六第6题(i))，但现在$p\equiv -1 \pmod 8$，矛盾；

(iii) 同(i)的论证。先证-3。若不然，-3是模p的二次剩余，$p\equiv 1 \pmod 6$(见第四章习题六第3题(i))，但现在$q=2k+1, p=4k+3$，仅当$k=3l+1$时才有$p\equiv 1 \pmod 6$，而这时$q=6l+3>3$—

定不是素数，矛盾。若 -4 不是原根，则 -4 是模 p 的二次剩余，即 -1 是二次剩余，$p\equiv1\pmod 4$，但这里 $p\equiv3\pmod 4$，矛盾；

(iv) 若2不是模 p 的原根，则 $2^4\equiv1\pmod p$，$2^{2q}\equiv1\pmod p$ 必有一成立。第一式显见不可能。若 $2^{2q}\equiv1\pmod p$，则 $2^q\equiv1\pmod p$ 或 $2^q\equiv-1\pmod p$。所以，2 或 -2 为模 p 的二次剩余，因此 $p\equiv\pm1,3\pmod 8$。但现在 $p\equiv5\pmod 8$，矛盾。

17. 即第15题(v)。

18. $\phi(p)=2q$. 模 p 的二次剩余一定不是原根。$p\equiv-1\pmod 8$，所以 -1 是二次非剩余。设 $a\not\equiv-1\pmod p$ 是二次非剩余。$a^{(p-1)/2}\equiv a^q\equiv-1\pmod p$，由此及 $\delta_p(a)|2q$ 推出 $\delta_p(a)=2q$，即 a 是原根。所以模 p 恰好有 $q-1\geqslant3$ 个原根。由 $p\equiv-1\pmod 8$ 知 $\left(\frac{2}{p}\right)=1$. 设 $q=4k+3$，由素数 $q>3$ 知 $3\nmid k$. 因而 $\left(\frac{3}{p}\right)=-\left(\frac{8k+7}{3}\right)=-\left(\frac{-1}{3}\right)=1$. 所以 2,3,4 均为二次剩余，因而，$-2$，$-3$，$-4$ 均是二次非剩余，即原根。

19. 设 $k=q\cdot\lambda+d$，$0\leqslant d<\lambda$. 由假设及 $a^{\phi(m)}\equiv b^{\phi(m)}\equiv1\pmod m$ 即证。

20. (i) 由上题推出；

(ii) 设 $p|a^n+b^n$. 若 $p|a$ 或 $p=2$ 则结论显然成立。若 $2<p\nmid a$，则 $p|c^n+1$，$c\equiv ab^{-1}\pmod p$. 设 λ 是使 $c^s\equiv-1\pmod p$ 成立的最小正整数 s，则 2λ 是使 $c^t\equiv1\pmod p$ 成立的最小正整数 t. 所以 $\lambda|n$ 及 $p\equiv1\pmod{2\lambda}$。若 $\lambda=n$，则 $p=2nk+1$；若 $\lambda<n$，设 $n=2^hn'$，$2\nmid n'$，这样，$\lambda=2^k\lambda'$，$2\nmid\lambda'$，$k\leqslant h$，$\lambda'|n'$. 若 $k<h$，则 $c^{2^kn'}\equiv-1\pmod p$。当 $h<k$ 时，$((c^{n'})^{2^k}+1,(c^{n'})^{2^h}+1)=1$ 或2，这不可能。所以必有 $k=h$。

(iii) 由(ii)推出。

21. $\delta_m(a)=(\delta_m(a),c)\cdot d$.

22. (i) $\delta_m(a^\lambda)=\delta_m(a)/\lambda$，$\delta_m(b^\lambda)=\delta_m(b)/\lambda$. 因此，$(\delta_m(a^\lambda),\delta_m(b^\lambda))=1$；(ii) 利用(i)及 $\delta_m((ab)^\lambda)=\delta_m(ab)/(\delta_m(ab),\lambda)$。

23. (i) $p\equiv 1(\bmod 4)$，所以恰有两解 $\pm x_0$. $\left(\frac{\pm x_0}{p}\right)=\left(\frac{x_0}{p}\right)$. $\left(\frac{x_0}{p}\right)=1$ 的充要条件是 $1\equiv x_0{}^{(p-1)/2}\equiv x_0{}^{2q}\equiv x_0^2(\bmod p)$，所以 $\left(\frac{x_0}{p}\right)=-1$；

(ii) 设 a 是二次非剩余，$a\not\equiv\pm x_0(\bmod p)$. $a^{(p-1)/2}\equiv a^{2q}\equiv -1(\bmod p)$. 由此及 $\delta_p(a)\mid 4q$ 就推出 $\delta_p(a)=4q$，即 a 是原根.

(iii) 模29的二次剩余是：$\pm 1,\pm 4,\pm 5,\pm 6,\pm 7,\pm 9,\pm 13$. $x^2\equiv -1(\bmod 29)$的两解是 ± 12. 因此原根是：$\pm 2,\pm 3,\pm 8,\pm 10,\pm 11,\pm 14$. 模 53 的二次剩余是：$\pm 1,\pm 4,\pm 6,\pm 7,\pm 9,\pm 10,\pm 11,\pm 13,\pm 15,\pm 16,\pm 17,\pm 24,\pm 25$. $x^2\equiv -1(\bmod 53)$ 的两解是 ± 23. 因此，原根是：$\pm 2,\pm 3,\pm 5,\pm 8,\pm 12,\pm 14,\pm 18,\pm 19,\pm 20,\pm 21,\pm 22,\pm 26$.

24. 设 $\delta_p(a)=\lambda$. $\lambda\mid 2^n q$. a 是二次非剩余的充要条件是 $a^{2^{n-1}q}\equiv -1(\bmod p)$. 由此及条件 $a^{2^n}\not\equiv 1(\bmod p)$ 推出 $\lambda=2^n q$.

25. 必有 $a^4\equiv 1(\bmod p)$, $a^2\equiv -1(\bmod p)$, $a^3\equiv -a(\bmod p)$. 所以 $(1+a)^4=a^4+4a^3+6a^2+4a+1\equiv -4(\bmod p)$. 最小正剩余为 $p-4$.

26. (i) $2^{17}-1$ 的素因数 $p=34k+1$. $(2^{17}-1)^{1/2}<363$. 以这种形式的不超过 363 的素数 $p=103,137,239,341$ 去试除；

(ii) 设素数 $p\mid(2^{19}+1)/3$. 易证 $p>3$, $2^{38}\equiv 1(\bmod p)$, $2^2\not\equiv 1(\bmod p)$, $2^{19}\not\equiv 1(\bmod p)$，所以，$38=\delta_p(2)\mid p-1$，即 $p=38k+1$. $((2^{19}+1)/3)^{1/2}=(174763)^{1/2}<419$. 不超过419的这种形式的素数 p 有：191, 229，通过试除即得。

27. 必有 k 使 $g^h\equiv g-1(\bmod p)$, $0\leqslant h\leqslant p-2$，取 $k=p-1-h$ 即可。

28. 若有这样的 k，则 $g^{k+1}(g-1)\equiv 1(\bmod p)$, $g^k(g-1)\equiv 1(\bmod p)$. 进而有 $g^k(g-1)^2\equiv 0(\bmod p)$. 这与 g 是原根矛盾。

29. 由性质 7 推出。

30. 利用上题及 $m\neq 3,4,6$ 时必有 $2|\phi(\phi(m))$。

31. (i) 即第 15 题(vi)的一部分；(ii) 若 m 是素数，则 $m=2^{2^h}+1$，$h\geqslant 1$. 在第 15 题(vi)的证明中已证，3 是模 m 的二次非剩余，所以必要性成立。若 $3^{(m-1)/2}\equiv -1(\bmod m)$，则 $3^{2^{n-1}}\equiv -1(\bmod m)$，$3^{2^n}\equiv 1(\bmod m)$，即 3 对模 m 的指数为 $m-1$。所以 m 为素数。

32. 这是第15题(vi)的一部分。

习　题　二

1. 见附表 1。

2. 依次可取：7,31,−3,−65,−338。

3. 直接计算；证明 $10^{486}\equiv 1(487^2)$。

4. 依次为3,7,3,3,3,−5,3,7。

5. 取 g 为模 p 原根. $1^k+\cdots+(p-1)^k\equiv\sum_{j=1}^{p-1}g^{kj}$. 由此及 $g^k\not\equiv 1(\bmod p)$ 当 $p-1\nmid k$，$g^k\equiv 1(\bmod p)$，当 $p-1|k$，就推出所要结论。

6. (i) 设 $1,2,\cdots,p-1$ 所可能取到的不同的指数是 $\delta_1,\cdots,\delta_s$. 我们有 $\tau=[\delta_1,\cdots\delta_s]|p-1$，设 τ 的素因数分解式是 $p_1^{\alpha_1}\cdots p_t^{\alpha_t}$. 必有 a_j 对模 p 的指数为 $p_j^{\alpha_j}(1\leqslant j\leqslant t)$。再证 $\tau=p-1$ 就推出了(i)。这可由 $x^\tau-1\equiv 0(\bmod p)$ 的解数为 $p-1$ 推出。

(ii) 由(i)及 § 1性质 8 就推出。

(iii) 2 的指数为11，−1的指数为 2，所以 −2是模23的原根。

7. 仅有 $n=1979$，是素数。

8. 7。

9. 利用第 1 题的结果，取 g 为模 p 最小正原根，再求 g^k 对模 p 的最小正剩余，$1\leqslant k\leqslant p-1$，$(k,p-1)=1$，即得. 模19为：2,3,10,13,14,15；模31为：3,11,12,13,17,21,22,24；模37为：2，5,13,15,17,18,19,20,22,24,32,35；模53为：2,3,5,8,12,

14,18,19,20,21,22,26,27,31,32,33,34,35,39,41,45,48,50,51；模71为：7,11,13,21,22,28,31,33,35,42,44,47,52,53,55,56,59,61,62,63,65,67,68,69。

10. 只要把上题为偶数的原根 g 改为 $g+p$。

11 对模 2^{α_0} 存在指数为 2^{c_0} 的数 a_0，对模 $p_j^{\alpha_j}$ 存在指数为 $\phi(p_j^{\alpha_j})$ 的数 a_j（即原根）。由此及§1性质10即得所要结论。

习 题 三

1. 由 $r_{23,11}(5)\cdot r_{23,5}(11)\equiv 1 \pmod{22}$ 得 $r_{23,11}(5)=5$。因而，$\gamma_{23,11}(a)\equiv 5\gamma_{23,5}(a) \pmod{22}$。

a	−11	−10	−9	−8	−7	−6	−5	−4	−3	−2	−1
$\gamma_{23,11}(a)$	12	4	17	19	18	13	16	9	3	21	11

a	1	2	3	4	5	6	7	8	9	10	11
$\gamma_{23,11}(a)$	0	10	14	20	5	2	7	8	6	15	1

2.

$\gamma_{13,2}(a)$	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

$\gamma_{17,3}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

$\gamma_{19,2}(a)$	0	1	2	3	4	5	6	7	8
a	1	2	4	8	16	13	7	14	9

$\gamma_{19,2}(a)$	9	10	11	12	13	14	15	16	17
a	18	17	15	11	3	6	12	5	10

$\gamma_{41,6}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a	1	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33

$\gamma_{41,6}(a)$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
a	34	40	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7

$\gamma_{47,5}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	5	25	31	14	23	21	11	8	40	12	13	18	43	27	41

$\gamma_{47,5}(a)$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
a	17	38	2	10	3	15	28	46	42	22	16	33	24	26	36

$\gamma_{47,5}(a)$	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
a	39	7	35	34	29	4	20	6	30	9	45	37	44	32	19

$\gamma_{53,2}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
a	1	2	4	8	16	32	11	22	44	35	17	34	15	30	7	14	28	3

$\gamma_{53,2}(a)$	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
a	6	12	24	48	43	33	13	26	52	51	49	45	37	21	42	31	9

$\gamma_{53,2}(a)$	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
a	18	36	19	38	23	46	39	25	50	47	41	29	5	10	20	40	27

$\gamma_{71,7}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
a	1	7	49	59	58	51	2	14	27	47	45	31	4	28	54	23	19	62

$\gamma_{71,7}(a)$	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
a	8	56	37	46	38	53	16	41	3	21	5	35	32	11	6	42	10	70

$\gamma_{71,7}(a)$	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
a	64	22	12	13	20	69	57	44	24	26	40	67	43	17	48	52	9	63

$\gamma_{71,7}(a)$	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
a	15	34	25	33	18	55	30	68	50	66	36	39	60	65	29	61

以上列出的 a 都是最小正剩余。

3. $-221\cdot 2^{\gamma^{(1)}}-51\cdot 2^{\gamma^{(2)}}+7\cdot 39\cdot 3^{\gamma^{(3)}}$, $0\leqslant\gamma^{(1)}\leqslant 2$, $0\leqslant\gamma^{(2)}\leqslant 12, 0\leqslant\gamma^{(3)}\leqslant 16$.

$\tilde{g}_1=-221\cdot 2-51+7\cdot 39=-220$,

$\tilde{g}_2=-221-51\cdot 2+7\cdot 39=50$,

$\tilde{g}_3=-221-51+7\cdot 39\cdot 3=547$ ($\tilde{g}_3$ 也可取 -116).

$(-220)^{\gamma^{(1)}}\cdot 50^{\gamma^{(2)}}\cdot 547^{\gamma^{(3)}}$, $0\leqslant\gamma^{(1)}\leqslant 2, 0\leqslant\gamma^{(2)}\leqslant 12$, $0\leqslant\gamma^{(3)}\leqslant 16$.

4. $-17\cdot 121\cdot 3^{\gamma^{(1)}}+42\cdot 49\cdot 7^{\gamma^{(2)}}$, $0\leqslant\gamma^{(1)}\leqslant 41$, $0\leqslant\gamma^{(2)}\leqslant 109$.

$\tilde{g}_1=-17\cdot 121\cdot 3+42\cdot 49=-4113$,

$$\bar{g}_2 = -17 \cdot 121 + 42 \cdot 49 \cdot 7 = 12349.$$

由于 $7^2 \cdot 11^2 = 5929$，可取 $\bar{g}_1 = 1816$，$\bar{g}_2 = 491$。

$$1816^{\gamma^{(1)}} \cdot 491^{\gamma^{(2)}},\quad 0 \leqslant \gamma^{(1)} \leqslant 41,\quad 0 \leqslant \gamma^{(2)} \leqslant 109.$$

5．$3 \cdot 43(-1)^{\gamma^{(-1)}} 5^{\gamma^{(0)}} + (-2) \cdot 64 \cdot 3^{\gamma^{(1)}}$，$0 \leqslant \gamma^{(-1)} \leqslant 1$，$0 \leqslant \gamma^{(0)} \leqslant 15$，$0 \leqslant \gamma^{(1)} \leqslant 41$。$\bar{g}_{-1} = 3 \cdot 43 \cdot (-1) + (-2) \cdot 64 = -257$，$\bar{g}_0 = 3 \cdot 43 \cdot 5 + (-2) \cdot 64 = 517$，$\bar{g}_1 = 3 \cdot 43 + (-2) \cdot 64 \cdot 3 = -255$，$(-257)^{\gamma^{(-1)}} 517^{\gamma^{(0)}} (-255)^{\gamma^{(1)}}$，$0 \leqslant \gamma^{(-1)} \leqslant 1$，$0 \leqslant \gamma^{(0)} \leqslant 15$，$0 \leqslant \gamma^{(1)} \leqslant 41$。

6．由原根定义推出，对任一原根 g 必有

$$g^{\phi(m)/2} \equiv -1 \pmod{m}.$$

7．

模 $32 = 2^5$ 的指标表

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7
a	1	5	25	29	17	21	9	13

$\gamma^{(-1)}(a)$	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7
a	31	27	7	3	15	11	23	19

模 $128 = 2^7$ 的指标表

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	5	25	125	113	53	9	45	97	101	121	93	81	21	105	13

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\gamma^{(0)}(a)$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
a	65	69	89	61	49	117	73	109	33	37	57	29	17	85	41	77

$\gamma^{(-1)}(a)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	127	123	103	3	15	75	119	83	31	27	7	35	47	107	23	115

$\gamma^{(-1)}(a)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
a	63	59	39	67	79	11	55	19	95	91	71	99	111	43	87	51

模 $256 = 2^8$ 的指标表

$\gamma^{(-1)}(a)$	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1 255	5 251	25 231	125 131	113 143	53 203	9 241	45 211	225 31	101 155	249 7	221 35	81 175	149 107	233 23	141 115

$\gamma^{(-1)}(a)$	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1
$\gamma^{(0)}(a)$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
a	193 63	197 59	217 39	61 195	49 207	245 11	201 55	237 19	161 95	37 219	185 71	157 99	17 239	85 171	169 87	77 179

$\gamma^{(-1)}(a)$	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1	0 1
$\gamma^{(0)}(a)$	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
a	129 127	133 123	153 103	253 3	241 15	181 75	137 119	173 83	97 159	229 27	121 135	93 163	209 47	21 235	105 151	13 243

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
a	65	69	89	189	177	117	73	109	33	165	57	29	145	213	41	205
	191	187	167	67	79	139	183	147	223	91	199	227	111	43	215	51

8. (i) 对 2^5 取 -1, 5; 对 29 取原根 2; 对 41^2 取原根 7. 3 的指标组为 $\{1,3;5,825\}$;

(ii) 对 2 取 -1, 5; 对 13, 23, 41, 47 依次取原根 2, 5, 6, 5. 3 的指标组为 $\{0,0;4,16,15,20\}$.

习 题 四

1. (i) 无解; (ii) $x\equiv 1,13,16,4 \pmod{17}$; (iii) $x\equiv 2 \pmod{17}$; (iv) $x\equiv -9 \pmod{23}$; (v) $x\equiv 29,3,30,13,7 \pmod{41}$; (vi) $x\equiv 4 \pmod{41}$; (vii) $x\equiv 7,18 \pmod{22}$; (viii) 无解.

2. 所有 a, $(a,19)=1$. **3.** $b\equiv 29,3,30,13,7 \pmod{41}$.

4. $x\equiv a \pmod{18}$, $x^{a-1}\equiv 1 \pmod{19}$, $1\leqslant a\leqslant 18$, $(x,19)=1$.

5. $x\equiv a \pmod{22}$, $x\equiv 5^a \pmod{23}$, $0\leqslant a\leqslant 21$.

6. -1 对模 p 任一原根的指标均为 $(p-1)/2$. 因此, $x^4\equiv -1 \pmod p$ 有解的充要条件是 $(4, p-1) | (p-1)/2$, 即 $p\equiv 1 \pmod 8$.

7. (i) $x\equiv \pm 9, \pm 23 \pmod{64}$; (ii) 无解.

8. (i) 无解; (ii) 无解.

9. 利用定理 2 的前一式即可写出全部三次、四次剩余.

10. 26 次剩余为 2^{26t}, $0\leqslant t< 106$.

11. 见第 6 题.

12. 设 g 是 p 的原根，$\gamma=\gamma_{p,g}(2)$。原同余方程等价于 $8y\equiv 4\gamma(\bmod p-1)$。当 $p\equiv\pm1(\bmod 8)$时，$2|\gamma$。

13. 设 $p-1=2^l\cdot c$，$2\nmid c$，由§3性质4及 $2\nmid\delta_p(a)$知，2^l 必整除 a 的指标（以任一原根 g 为底）。由此及 -1 的指标为 $(p-1)/2$，即可推出所要结论。

14. $x\equiv 1,6(\bmod 10)$。

15. $a\equiv1,10,16,18,37(\bmod 41)$。

16. $\delta_{73}(2)=9$。由定理3及式(8)推出。

17. (i) 即 $(x^2-2)(x^2+2)\equiv0(\bmod 37)$。$\left(\frac{-2}{37}\right)=\left(\frac{2}{37}\right)=-1$，无解；

(ii) $x\equiv10,33,31,8(\bmod 41)$。

18. 原方程即 $x^4+x^3+x^2+x+1\equiv0(\bmod 41)$，$x\equiv1(\bmod 41)$不是解，所以原方程的解是$x^5\equiv1(\bmod 41)$的解去掉$x\equiv1(\bmod 41)$。即 $x\equiv10,18,16,37(\bmod 41)$。

19. 必要性显然。若 $\left(\frac{a}{p}\right)=1$，则 $a\equiv b^2(\bmod p)$。$x^4-a\equiv(x^2-b)(x^2+b)(\bmod p)$。

当 $p\equiv3(\bmod 4)$时，$\left(\frac{b}{p}\right)$，$\left(\frac{-b}{p}\right)$必有一个为1。

第 六 章

习 题 一

1. 证法同引理3。

4. (i) $23\cdot53=27^2+15^2+12^2+11^2=25^2+19^2+13^2+8^2$；

(ii) $43\cdot197=74^2+51^2+15^2+13^2=69^2+57^2+19^2+10^2$；

(iii) $47\cdot223=101^2+12^2+10^2+6^2=77^2+54^2+40^2+6^2$。

5. x,y,z 一定是两奇一偶。

6. 当 $N-1$ 不等于 0,1,2,3,4,6,7,9,10,12,15,18,33 时，由定理 7 知N一定可表为六个正平方和。$34=3^2+3^2+2^2+2^2+2^2+2^2$。再直接验证：仅当 $N=1,2,3,4,5,7,8,10,11,13,16,19$时不能表为六个正平方和。

7. 用归纳法证第一个结论。$k=0$ 时结论成立。假设$k=n$ $(\geqslant 0)$时成立。当 $k=n+1$ 时，若 $2^{n+1}=x_1^2+x_2^2+x_3^2, x_1>0, x_2>0, x_3>0$，则 x_1,x_2,x_3 一定是两奇一偶.且两个奇数不能相等。由此推出矛盾。当 $k>2, 2^k=x_1^2+x_2^2+x_3^2+x_4^2, x_i$ 一定全为偶数。因此,$2^{2k}=(2^{k-1})^2+(2^{k-1})^2+(2^{k-1})^2+(2^{k-1})^2, 2^{2k+1}=(2^k)^2+(2^k)^2+0^2+0^2$.

8. 由上题推出。

习 题 二

1. 1,2,4,5,8,9,10,13,16,17,18,20,25,26,29,32,34,36,37,40,41,45,48,49,50,52,53,58,61,64,65,68, 72, 73, 74, 80, 81,82,85,89,90,97,98 可表为两平方数之和，其它则不能。

2. 设 $c^2\equiv -1 \pmod p$。必有 $a\equiv cb$ 或 $-cb \pmod p$，$a_1\equiv cb_1$ 或 $-cb_1 \pmod p$。$p^2=(aa_1\pm bb_1)^2+(ab_1\mp ba_1)^2$，右边必有一为零。

3. (i) $5\cdot 13=8^2+1^2=7^2+4^2$； (ii) $17\cdot 29=22^2+3^2=18^2+13^2$； (iii) $37\cdot 41=34^2+19^2=29^2+26^2$； (iv) $5\cdot 13\cdot 17\cdot 29=179^2+2^2=173^2+46^2=178^2+19^2=163^2+74^2=157^2+86^2=131^2+122^2=166^2+67^2=142^2+109^2$； (v) $7^2\cdot 13\cdot 17=(7\cdot 14)^2+(7\cdot 5)^2=(7\cdot 11)^2+(7\cdot 10)^2$。

4. 由定理 2 推出。

5. 利用第 4 题证明。

6. (i) 充分性显然。必要性由第 5 题或第 4 题推出；(ii) 利用定理 2，由(i)推出。

7. n 不能有 $4k+3$ 形式的素因数。

8. 即第四章习题六第33题。

9. (i) 设 $p=4m+1$，$S(k)=2\sum_{j=1}^{2m}\left(\frac{j(j^2+k)}{p}\right)$；

(ii) 当 $p|l$ 时，$S(kl^2)=\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)=0$，当 $p\nmid l$ 时，

$$S(kl^2)=\sum_{j=0}^{p-1}\left(\frac{jl((jl)^2+kl^2)}{p}\right).$$

10. 由 $\left(\frac{ab}{p}\right)=-1$ 直接推出这 $p-1$ 个数两两不同余。

11. (i)

$$q(S(a))^2+q(S(b))^2=\sum_{l=1}^{q}(S(al^2))^2+\sum_{l=1}^{q}(S(bl^2))^2$$

$$=\sum_{k=1}^{p-1}(S(k))^2;$$

(ii) 利用第 8 题；(iii)由(ii) 得 $q(S(a))^2+q(S(b))^2=4pq$，再利用第 9 题(i)。

13. 证法和定理 4 相同。

14. 不适用，充分性证明的最后一部分在这里可能不成立。例如，$p=7$ 时，$\left(\frac{-5}{7}\right)=1$，但 $7=x^2+5y^2$ 无解。

15. 取 $(x-\sqrt{d}\,y)=(x_1-\sqrt{d}\,y_1)(x_2-\sqrt{d}\,y_2)$ 即可。

16. (i)利用定理 4 和上题；(ii)利用第13,15题。

18. 原方程可写为 $4p=(2x-y)^2+3y^2$，再利用定理 4 。

19. 利用上题，及 $a,b,a-b$ 总可设法使其中一个被 3 整除。

习 题 三

2.

n	200	201	202	203
$N(n)$	12	0	8	0
$P(n)$	0	0	2	0
$Q(n)$	0	0	8	0

4．设 $n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}\ q_1^{\beta_1}\cdots q_s^{\beta_s}$，$p_i\equiv 1 \pmod 4$，$q_i\equiv 3 \pmod 4$．$n$ 和 $n'=n/2^{\alpha_0}$ 的奇正除数个数相同．比较 $n''=q_1^{\beta_1}\cdots q_s^{\beta_s}$ 的形如 $4k+1$ 的正除数和形如 $4k+3$ 的正除数个数．

5．即 $R(n)$ 等于零的充要条件．

6．当 $n\equiv 1 \pmod 4$ 时，$u^2+v^2=n$ 的两个解对应于 $4x^2+y^2=n$ 的一个解．

7．利用上题，及§3对 $N(n),Q(n),P(n)$ 的讨论结果．

10．(i) 对 $s\neq t$ 的那些项，这样两两聚项 $\{s,t,x,y\},\{s',t',x',y'\}$：设 $l=[t/(s-t)]$，$x'=-ls+(l+1)t$，$y'=(l+1)s-(l+2)t$，$s'=(l+2)x+(l+1)y$，及 $t'=(l+1)x+ly$．必有

$$h(st)+h(s't')=0;$$

(ii) 若 $2n=x_1^2+x_2^2+x_3^2+x_4^2$，则这些 x_i 是两偶两奇．因此，x_1,x_2 为偶，x_3,x_4 为奇的解数是 $N_4(2n)/6$．而由这组解可得 $n=y_1^2+y_2^2+y_3^2+y_4^2$ 的解：$y_1=(x_1+x_2)/2$，$y_2=(x_1-x_2)/2$，$y_3=(x_3+x_4)/2$，$y_4=(x_3-x_4)/2$，且满足 $2\mid y_1+y_2$，$2\nmid y_3+y_4$．由此推出 $N_4(2n)/6\leqslant N_4(n)/2$．类似可证 $N_4(n)/2\leqslant N_4(2n)/6$．这就证明了 $N_4(2n)=3N_4(n)$．若 $4n=x_1^2+x_2^2+x_3^2+x_4^2$ 则 x_i 或全为偶或全为奇，利用上面的变换，可建立与 $2n=y_1^2+y_2^2+y_3^2+y_4^2$ 的解之间一一对应，这就推出 $N_4(2n)=N_4(4n)$．由对 $4n$ 的解的讨论，利用(i)及定义就推出 $N_4(4n)$ 的公式．

习　题　四

1．(i) 无解；(ii) 有解，$x=1$，$y=1$，$z=2$；(iii) 无解；(iv) 有解，$x=5$，$y=2$，$z=1$；(v) 无解；(vi) 有解，

$x=y=1, z=2$。

第七章

习题一

1. (i) 10/7；渐近分数是：1,3/2,10/7；

(ii) 7/10；渐近分数是：0,1,2/3,7/10；

(iii) 10/3；渐近分数是：3,7/2,10/3；

(iv) 51/20；渐近分数是：2,3,5/2,23/9,28/11,51/20；

(v) −683/187；渐近分数是：−4，−7/2，−11/3，−84/23，−683/187；

(vi) −5/7；渐近分数是：−1,1,−5/7；

(vii) 1193/322；渐近分数是：1/2,9/2,41/66,1193/322。

2. (i) <5,1,3,5>；(ii) <−1,2,1,9>；(iii) <0,1,1,1,1,5,1,8>；(iv) <0,5,1,1,2,1,4,1,21>。

3. 2,3,2+2/3，2+3/4，2+5/7，2+23/32，2+28/39，2+51/71,2+334/465,2+385/536,2+719/1001，2+3799/5289 =2.718283229。e 的近似值是：2.718281828…。这个连分数是 e 的无限简单连分数展开的一个渐近分数。

6. 由式(37),(38)推出。

7. (i) 利用式(37),用归纳法证；(ii) 利用(i),及式(42)。

8. 由式(42)推出。

9. 利用式(37),(38),用归纳法证。

10. 用归纳法证，利用式(37),(38)。由此，亦推出第9题。

11. 利用式(37),(38)，用归纳法证，这里 P_n, Q_n 均看作是多项式。

12. 利用式(39),(40)，及式(29)—(33)，即可推出。

习 题 二

1. 由式(4)及(5)推出。

2. (i) $205/93=\langle 2,93/19\rangle=\langle 2,4,19/17\rangle=\langle 2,4,1,17/2\rangle=\langle 2,4,1,8,2\rangle$. $\langle 2,4,1,8\rangle=\langle 2,4,9/8\rangle=\langle 2,44/9\rangle=97/44$. 由第1题知，$205\cdot 44-93\cdot 97=-1=-(205,93)$，所以解为$x=-44+93t$, $y=97-205t$, $t=0,\pm 1,\pm 2,\cdots$. 其它各题用同样方法求解。(iv) 无解。

3. (i) $\langle 0,1,1,1,3\rangle=\langle 0,1,1,1,2,1\rangle$;

(ii) $\langle 3,6,1,7\rangle=\langle 3,6,1,6,1\rangle$;

(iii) $\langle -1,1,22,3,1,1,2,2\rangle=\langle -1,1,22,3,1,1,2,1,1\rangle$;

(iv) $\langle 1,2,1,4,3,1,5,2,1,3\rangle=\langle 1,2,1,4,3,1,5,2,1,2,1\rangle$;

(v) $\langle -1,1,3,1,1,2,1,4,1,21\rangle=\langle -1,1,3,1,1,2,1,4,1,20,1\rangle$.

4. (i) $a_i=b_i$, $0\leqslant i\leqslant n-1$, $a_n=b_n+1$, $b_{n+1}=1$;

(ii) 充要条件是：(Ⅰ) $a_i=b_i$, $0\leqslant i\leqslant n$, $2|n$; 或(Ⅱ) 存在 r, $0\leqslant r\leqslant n$, 使 $a_i=b_i$, $0\leqslant i<r$, $a_r\neq b_r$, 这时还分三种情形：(a) $r\neq n, 2\nmid r, a_r>b_r$; (b) $r\leqslant n, 2|r, a_r<b_r$; 或 (c) $r=n$, $2\nmid n$, 当 $b_{n+1}>1$ 时, $a_n>b_n$; 当 $b_{n+1}=1$时, $a_n>b_{n+1}$.

5. 利用第 1 题及习题一第 6 题 (ii)可得：若结论成立，则有 $ak_{n-1}=b^2+(-1)^{n+1}$. 这就推出了必要性。当条件(i)或(ii)成立时，由第 1 题可推出：$a|b-h_{n-1}$，即 $h_n|k_n-h_{n-1}$. 由此推出 $b=k_n=h_{n-1}$. 因而，由习题一第 6 题就证明了充分性。

6. 利用 § 1定理 2，适当选取 a/c 的连分数表示式。

习 题 三

1. (i) $(25-\sqrt{5})/10$; (ii) $(4+\sqrt{37})/7$;

(iii) $(\sqrt{21}-1)/10$; (iv) $-3+\sqrt{2}$.

3. (i) $\sqrt{7}=\langle 2,\overline{1,1,1,4}\rangle$; (ii) $\sqrt{13}=\langle 3,\overline{1,1,1,6}\rangle$;

(iii) $\langle 5,\overline{2,1,1,2,10}\rangle$；　(iv) $(\sqrt{10}+1)/3=\langle\overline{1,2,1}\rangle$；

(v) $(5-\sqrt{37})/3=\langle -1,1,1,\overline{1,3,2}\rangle$。

4．利用式(8)，及§1定理1．

6．利用习题二第6题。

9．必有唯一 $n\geqslant 0$，使 $k_n\leqslant b<k_{n+1}$，再利用定理6(i)。

11．必有唯一的 $n\geqslant 0$ 使 $k_n\leqslant b<k_{n+1}$。若 $b=k_n$，则利用定理6(ii)；若 $k_n<b<k_{n+1}$，则利用证定理6的方法讨论，考虑 $\xi_0=\sqrt{2}$，说明对它的第二渐近分数不一定有（＊＊）成立。

13．设 $\beta=\langle b_1,b_2,\cdots\rangle$，$\eta_n=\langle a_0,\cdots,a_n,\beta\rangle$，再利用§1定理2及§2定理1。

习　题　四

1．(ii) 利用§3定理7，§3式(18)，及(i)。

2．设 $\xi_0=\langle a_0,a_1,\cdots\rangle$，$\lambda(\xi_0,n)=\xi_{n+1}+k_{n-1}/k_n$。利用习题一第6题可得 $k_n/k_{n-1}=\langle a_n,\cdots,a_1\rangle,n\geqslant 1$。由此来计算 $\lambda(\xi_0,n)$，$n\geqslant 0$，进而从式(4)就可推出本题所要的结论。

$\xi_0=\sqrt{2}=\langle 1,\overline{2}\rangle$。对所有的渐近分数，当 $\lambda=2,\sqrt{5}$ 时，式(2)都成立，$\lim\limits_{n\to\infty}\lambda(\xi_0,n)=2\sqrt{2}$。

$\xi_0=(\sqrt{5}+1)/2=\langle\overline{1}\rangle$。对 $h_n/k_n(n\geqslant 1)$，当 $\lambda=2$ 时式(2)成立；对 h_n/k_n $(2\nmid n\geqslant 1)$，当 $\lambda=\sqrt{5}$ 时式(2)成立，$\lim\limits_{n\to\infty}\lambda(\xi_0,n)=\sqrt{5}$。

$\xi_0=\sqrt{11}=\langle 3,\overline{3,6}\rangle$。对所有的 h_n/k_n，当 $\lambda=2,\sqrt{5}$ 时，式(2)都成立，$\lim\limits_{m\to\infty}\lambda(\xi_0,2m+1)=2\sqrt{11}$，$\lim\limits_{m\to\infty}\lambda(\xi_0,2m)=\sqrt{11}$ 是两个极限点，上极限是 $2\sqrt{11}$。

$\xi_0=\sqrt{14}=\langle 3,\overline{1,2,1,6}\rangle$。对 h_n/k_n $(n\equiv 1,3(\bmod 4)$，当 $\lambda=2,\sqrt{5}$ 时式(2)都成立，四个极限点是：$\lim\limits_{m\to\infty}\lambda(\xi_0,4m)=2\sqrt{14}/5$，$\lim\limits_{m\to\infty}\lambda(\xi_0,4m+1)=\sqrt{14}$，$\lim\limits_{m\to\infty}\lambda(\xi_0,4m+2)=\sqrt{14}/5$，$\lim\limits_{m\to\infty}\lambda(\xi_0,$

$4m+3)=2\sqrt{14}$。上极限是$2\sqrt{14}$（本题可参看习题五第 1 题）。

3．对$\alpha=\xi_0$一定存在唯一的n使$k_n<x\leqslant k_{n+1}$。取a/b为h_n/k_n即满足要求。

4．(i) 先取定$n_0\geqslant 1$，及适当选取$a_0,\cdots,a_{n_0}$，使$k_{n_0}^{c-2}-2\geqslant 3$。然后依次选取正整数$a_{n+1}(n\geqslant n_0)$满足$a_{n+1}+2\leqslant k_n^{c-2}$。$\xi_0=\langle a_0,a_1,\cdots,a_n,\cdots\rangle$就满足要求；

(ii) $c\leqslant 2$即定理 1，因此可设$c>2$。只要取$a_{n+1}>k_n^{c-2}$，所得的$\xi_0=\langle a_0,a_1,\cdots,a_n,\cdots\rangle$就满足要求；

(iii) 必要性即定理 8，充分性用反证法。若$\xi_0=u/v$，则存在$b_n\to+\infty$，$a_n/b_n\neq u/v$，满足$1/b_n^2>|u/v-a_n/b_n|\geqslant 1/|vb_n|$，这不可能。

5．(i) 用归纳法证。第$n+1$行中的任意两个相邻分数（从左到右）必为以下三种情形之一：（Ⅰ）a/b，a'/b'；（Ⅱ）a/b，$(a+a')/(b+b')$；（Ⅲ）$(a+a')/(b+b')$，a'/b'，其中a/b，a'/b'是第n行中的两个相邻分数（从左到右）；

(ii) 由(i)推出；　　(iii) 由(i)推出；

(iv) 利用等式$a'/b'-a/b=(a'/b'-x/y)+(x/y-a/b)$，从(i)即可推出，进一步可证若$y=b+b'$，则必有$x=a+a'$；

(v) 用归纳法证。对$m/(n+1)$ $0<m<n+1,(m,n+1)=1$，必有第n行中的两个相邻分数$a/b,a'/b'$，满足$a/b<m/(n+1)<a'/b'$。由此及(iv)推出$n+1=b+b',m=a+a'$。

6．利用第 5 题 (i),(iv)及(v)。

7．利用第 6 题，第二部分要用ξ的无理性。

8．(i) 利用第 5 题(i)，证法同定理1；(ii) 利用第 5 题(i)，证法同定理 3 。

9．用归纳法证。

10．(i) 由第 5 题(v)推出；(ii) 由第 5 题(v)推出；(iii) 由第 5 题(i)推出；(iv) 利用第 5 题(i)，$0,1/n,1/(n-1)$是第n阶

Farey 数列中的三个相邻分数，当 $n\geqslant 2$ 时，$b_j\neq b_{j+1}$。

11.（i）不妨设 $b=n$，若不相邻，则必有 n 阶 Farey 分数 x_1/y_1，x_2/y_2，使 $a/b\geqslant x_1/y_1>x_2/y_2>c/d$，$x_1/y_1, x_2/y_2, c/d$ 是三个 n 阶 Farey 数列中的相邻分数，由此得 $1/(bd)\geqslant 1/(y_1y_2)+1/(y_2d)$，但这和 $y_2\leqslant n$ 矛盾。

（ii）取 $a/b=1/n$，$c/d=0/1$。

12. 利用第 5 题（iv）。

习 题 五

1.（i）利用习题一第 6 题；

（ii）利用（i），以及对任一取定的 j，$0\leqslant j\leqslant l-1$，当 $n\equiv m_0+j(\mathrm{mod}\,l)$，$n\to\infty$ 时，$\xi_{n+1}+k_{n-1}/k_n$ 的极限为 λ_{m_0-j}；

（iii）$\langle 2,5,1,\overline{1,2}\rangle$ 的两个极限点是：$\langle\overline{1,2}\rangle+(\langle\overline{2,1}\rangle)^{-1}=\sqrt{3}$，$\langle\overline{2,1}\rangle+(\langle\overline{1,2}\rangle)^{-1}=2\sqrt{3}$；$\langle 0,5,8,6,\overline{1,1,1,4}\rangle$ 的四个极限点是：$2\sqrt{7}/3, \sqrt{7}, 2\sqrt{7}/3, 2\sqrt{7}$（这里 $2\sqrt{7}/3$ 两个极限点相重）；$\langle 2,1,3,\overline{1,2,8}\rangle$ 的六个极限点是：$2\sqrt{19}/3, 2\sqrt{19}/5, \sqrt{19}, 2\sqrt{19}/5, 2\sqrt{19}/3, 2\sqrt{19}$（有四个不同的）。可以证明：这 l 个极限点是 $\langle\overline{a_k,\cdots,a_{k+l-1}}\rangle$ $(k=m_0+l,\cdots,m_0+2l-1)$ 的无理部分的两倍。

2.（i）$\langle 3,\overline{1,2}\rangle$；（ii）$\langle 6,\overline{1,1,3,1,5,1,3,1,1,12}\rangle$；

（iii）$\langle 1,1,3,1,5,1,3,1,1,\sqrt{43}+6\rangle=\langle\overline{1,1,3,1,5,1,3,1,1,12}\rangle$；

（iv）$\langle\overline{16,1}\rangle$；（v）$\langle 2,\overline{1,4,1,1}\rangle$；（vi）$\langle 2,\overline{3,1,1,3,4}\rangle$。

3.（i）$b=1,2,\cdots,2[\sqrt{d}]$；（ii）$a=[\sqrt{d}]$；（iii）$b=[\sqrt{d}],[\sqrt{d}]+1$。

5. 记 $\eta_0=-1/\xi_0'$。$\xi_0=(h_n\xi_0+h_{n-1})/(k_n\xi_0+k_{n-1})$，$\eta_0=(h_n\eta_0+k_n)/(h_{n-1}\eta_0+k_{n-1})$。利用习题一第 6 题。

6. $[\sqrt{d}]+\sqrt{d}$ 和 $\sqrt{d}$ 的周期相同，且前者是纯循环连分数。由 $[\sqrt{d}]+\sqrt{d}=\langle\overline{2[\sqrt{d}]}\rangle$ 可推出必要性。

10．同第6题的论证方法，由$[\sqrt{d}]+\sqrt{d}=\langle\overline{2[\sqrt{d}],b}\rangle$，$b\neq 2[\sqrt{d}]$，可推出必要性。

11．设$c_1=2$，$c_2=5$，及$c_s=2c_{s-1}+c_{s-2}$，$s\geqslant 3$。当取$d=(uc_s+1)^2+2c_{s-1}+1$时，$\sqrt{d}$的周期为$s+1$，这里u是任一正整数。$\sqrt{d}=\langle(uc_s+1),\overline{2,\cdots,2,2(uc_s+1)}\rangle$，其中有$s$个2。

12．利用第5题，取$\xi_0=[\sqrt{d}]+\sqrt{d}$。$-1/\xi_0'=1/(\sqrt{d}-[\sqrt{d}])=\langle\overline{a_1,\cdots,a_{l-1},2[\sqrt{d}]}\rangle$。但由第5题知，$-1/\xi_0'=\langle\overline{a_{l-1},\cdots,a_1,2[\sqrt{d}]}\rangle$。

13．(i) 由§2式(5)知，从方程组$ah_0+bk_0=h_l$，$ah_1+bk_1=h_{l+1}$可确定整数a,b；从方程组$ch_0+dk_0=k_l$，$ch_1+dk_1=k_{l+1}$可确定整数c,d。这些a,b,c,d即为所求；类似证(ii)。

14．用归纳法（对j）证式(*)及(**)。在证(**)时要利用以下关系式：设$\xi_0=[\sqrt{d}]+\sqrt{d}=\langle\overline{a_0,a_1,\cdots,a_{l-1}}\rangle$。由$\xi_{ml+1}=\xi_1$可得

$$\xi_0=(h_{ml}+h_{ml-1}(\xi_0-a_0))/(k_{ml}+k_{ml-1}(\xi_0-a_0)).$$

进而推出：

$$\begin{cases} h_{ml-1}=k_{ml}-a_0k_{ml-1}, \\ dk_{ml-1}=h_{ml}+a_0h_{ml-1}. \end{cases}$$

在式(*),(**)中以$2m,ml$代替m,j，并利用上式及式(38)（$l|n$及定理8(i)），就推出(***)。

15．α是二次方程$x^2-a_0x-c=0$的正根，即

$$\alpha=(a_0+\sqrt{a_0^2+4c})/2.$$

记$u_n=(\alpha^n-\beta^n)/(\alpha-\beta)$，$p_n=c^{-[(n+1)/2]}u_{n+2}$，$q_n=c^{-[(n+1)/2]}\cdot u_{n+1}$。用归纳法证明所要的结论：先证明当$n=-2,-1$时有$h_n=p_n$，$k_n=q_n$成立，然后证明：$h_n,p_n$满足同样的递推公式，$k_n,q_n$也满足同样的递推公式。

16．上题的特例，取$\alpha=(\sqrt{5}+1)/2$。

习 题 六

1. 见附表 2。

2. 见附表 2。

3. 考虑 Pell 方程 $x^2-a^2dy^2=1$ 的解。

4. 原方程可写为 $(2x+1)^2-2y^2=-1$。本题是求两直角边为相邻整数的商高三角形。

5. 即解不定方程 $n(n+1)=2y^2$，即 $(2n+1)^2-8y^2=1$。

6. (i) 可由 $x_{n+1}+y_{n+1}\sqrt{2}=(x_n+y_n\sqrt{2})(1+\sqrt{2})$ 推出；

(ii) 由 $x_{2n+1}+y_{2n+1}\sqrt{2}=(x_n+y_n\sqrt{2})(x_{n+1}+y_{n+1}\sqrt{2})$ 及(i) 推出；

(iii) $1+\sqrt{2}$ 是 $u^2-2v^2=-1$ 的最小正解，一般解是 $(u+v\sqrt{2})^{2n+1}$。另一方面，由第4题知，$v^2=((u+1)/2)^2+((u-1)/2)^2$，因此，$y_{2n+1}^2=((x_{2n+1}+1)/2)^2+((x_{2n+1}-1)/2)^2$；

(iv) 利用 $x_m^2-2y_m^2=(-1)^m$，及 $(x_n+y_n\sqrt{2})=(x_m+y_m\cdot\sqrt{2})(x_{n-m}+y_{n-m}\sqrt{2})$ 推出；

(v) 由 $x_{2n+1}+y_{2n+1}\sqrt{2}=(x_{n+1}+y_{n+1}\sqrt{2})(x_n+y_n\sqrt{2})$ 及 (iv) 推出；

(vi) 由 $x_{2n}+y_{2n}\sqrt{2}=(x_n+y_n\sqrt{2})^2$ 推出 $y_{2n}=2x_ny_n$，进而由此及 (ii) 推出所要结论。这也可直接从二项展开看出，且总有 $2\nmid x_n$；

(vii) 由 $x_n^2-2y_n^2=(-1)^n$ 知，这要证明 $u^4-2v^2=\pm1$，除了 $u=v=1$ 外无其它正整数解。$u^4-2v^2=1$ 可改写为 $(u^2-1)(u^2+1)=2v^2$，显见，它无正整数解。$u^4-2v^2=-1$ 可改写为 $u^4+(v^2-1)^2=v^4$，由第二章习题二第15题就推出它除了 $u=v=1$ 外无其它正整数解。

7. 设 $x_2+y_2\sqrt{p}$ 是 $x^2-py^2=1$ 的最小正解。由 $py_2^2=(x_2^2-1)$ 推出 $2\nmid x_2$，$2|y_2$，及 p 能且只能整除 x_2+1，x_2-1 中的一个。

因而有 $x_2\pm1=2x_1^2$，$x_2\mp1=2py_1^2$ 成立。进而得 $x_1^2-py_1^2=\pm1$。但 $x_2+y_2\sqrt{p}$ 是最小正解，$y_1<y_2$，所以只能取负号。

8. s,t 是 $x^2-dy^2=-1$ 的最小正解的充要条件是 $(s+t\sqrt{d})^2=u+v\sqrt{d}$。

9. 由§4定理8知存在无穷多对正整数满足 $|x-y\sqrt{d}|<1/y$. 由此及 $|x+y\sqrt{d}|\leqslant|x-y\sqrt{d}|+2y\sqrt{d}$，即得结论。

10. 由上题知，存在无穷多对 x,y，使 $|x^2-dy^2|$ 只取小于 $1+2\sqrt{d}$ 的有限个正整数值，因此，必有无穷多对 x,y，使 $x^2-dy^2=m$，$|m|<1+2\sqrt{d}$，由于 d 不是平方数，$m\neq0$。

11. (i) 由上题知必有不同的正整数对 x_1,y_1；x_2,y_2 满足：$x_1\equiv x_2(\bmod m)$，$y_1\equiv y_2(\bmod m)$，$x_1^2-dy_1^2=x_2^2-dy_2^2=m$。显见 $x_1\neq x_2$，$y_1\neq y_2$，由关系式 $(x_2+y_2\sqrt{d})=(x_1+y_1\sqrt{d})(u+v\sqrt{d})$ 可定出整数 u,v。再证明 $v\neq0$，$|u|+|v|\sqrt{d}$ 是解。这就证明了 (i)。

(ii) 用反证法证。设 $x+y\sqrt{d}$ 是一个正解，若结论不成立，则有 $(x_1+y_1\sqrt{d})^n<x+y\sqrt{d}<(x_1+y_1\sqrt{d})^{n+1}$，$n$ 为某一正整数。进而，$u+v\sqrt{d}=(x+y\sqrt{d})(x_1-y_1\sqrt{d})^n$ 也是正解，且 $u+v\sqrt{d}<x_1+y_1\sqrt{d}$。矛盾。

12. 设 $x_1+y_1\sqrt{d}$ 是 $x^2-dy^2=1$ 的正解，u_1,v_1 是原不定方程的解。那么 $(x_1+y_1\sqrt{d})^n(u+v\sqrt{d})=(u_n+v_n\sqrt{d})(n=1,2,\cdots)$ 所给出的 u_n,v_n 都是原方程的解。

14. 这时有 $|h-k\sqrt{d}|=|c|/|h+k\sqrt{d}|$。先假定 c 是正实数，满足 $0<c<\sqrt{d}$。这时有 $h>k\sqrt{d}$，因此，$|h-k\sqrt{d}|<1/2k$，因而由§3定理7推出结论成立. 若 c 是负的，则 $k^2-(1/d)h^2=-c/d$。因而有 $|k-h\sqrt{1/d}|=|c/d|/|k+h\sqrt{1/d}|$，由此及 $k>h\sqrt{1/d}$ 推出：$|k-h\sqrt{1/d}|<1/(2h)$。因而由§3定理7知 k/h 是 $1/\sqrt{d}$ 的渐近分数，即 h/k 是 $\sqrt{d}$ 的渐近分数（为什么）。

15. $\eta=1$ 时结论成立. 设 $\eta>1$. 用反证法. 设 $x_0+y_0\sqrt{d}$ 是最小正解，$1\leqslant y_1<\eta$。我们有 $x_1^2\eta^2-y_1^2\xi^2=\eta^2-y_1^2>0$。进而得：

$$x_1\eta + y_1\xi = c_1 > 0, \quad x_1\eta - y_1\xi = c_2 > 0,$$

$$c_1c_2 = \eta^2 - y_1^2.$$

由此推出 $\xi \leqslant \eta^2/2 - 1$。矛盾。

第 八 章

习 题 一

1. $\pi(200) = 46$, $\pi(300) = 62$, $\pi(400) = 78$, $\pi(500) = 95$, $\pi(600) = 109$, $\pi(700) = 125$, $\pi(800) = 139$, $\pi(900) = 154$, $\pi(1000) = 168$。

3. 0，因为 $n, n+1, n+2, n+3$ 中必有一数被 4 整除。

4. $\mu(1) + \mu(2) + \mu(6) = 1$。

5.

k	4	8	1	14	2	33	29
$\mu(k) + \mu(k+1) + \mu(k+2)$	0	1	-1	2	-2	3	-3

6. $n = m^2n_1, \mu(n_1) \neq 0$. $\sum\limits_{d^2 \mid n} f(d) = \sum\limits_{d \mid m} f(d)$. 再利用引理3。

7. (i) 类似式（27）可证：

$$\sum_{d \mid n} \mu^2(d) = \left(\sum_{i_1=0}^{\alpha_1} \mu^2(p_1^{i_1})\right) \cdots \left(\sum_{i_r=0}^{\alpha_r} \mu^2(p_r^{i_r})\right),$$

这里 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$；

(ii) $\sum\limits_{d \mid n} \mu(d)\tau(d)$

$$= \left(\sum_{i_1=0}^{\alpha_1} \mu(p_1^{i_1})\tau(p_1^{i_1})\right) \cdots \left(\sum_{i_r=0}^{\alpha_r} \mu(p_r^{i_r})\tau(p_r^{i_r})\right).$$

8. $n=m^k n_1$，对任一素数 $p, p^k \nmid n_1$。$d^k|n \Leftrightarrow d|m$。

9. 利用第 7 题的方法，并注意当且仅当 $p=2$ 时 $\phi(p)=1$。

10. $d|n=n_1n_2$，$(n_1,n_2)=1$ 的充要条件是 $d=d_1d_2$，$d_1=(d, n_1)$，$d_2=(d,n_2)$。

11. n。

12. (i) 由 $\phi(n)$ 的定义推出。

(ii) $\sum_{d=1}^{n} f((d,n)) = \sum_{k|n} \sum_{\substack{d=1 \\ (d,n)=k}}^{n} f((d,n))$。

(iii) 由(ii)得和式 $= \sum_{d|n} d\mu(d)\phi(n/d)$。$n=1$ 时等于 1. $n>1$ 时利用证第10题的方法，可证：当 $(n_1,n_2)=1$时，

$$\sum_{d|n_1n_2} d\mu(d)\phi(n_1n_2/d) = \sum_{d_1|n_1} d_1\mu(d_1)\phi(n_1/d_1) \cdot \sum_{d_2|n_2} d_2\mu(d_2)\phi(n_2/d_2).$$

由此及

$$\sum_{d|p^\alpha} d\mu(d)\phi(p^\alpha/d) = \begin{cases} -1, & \text{当 } \alpha=1; \\ 0, & \text{当 } \alpha>1, \end{cases}$$

即得所要结论。

13. 右边和式 $= \sum_{d=1}^{n} e^{2\pi i d/n} \sum_{k|(d,n)} \mu(k)$，再交换求和号。

14. 左边和式 $= \sum_{d\le x} \mu(d) \sum_{\substack{k\le x \\ d|k}} 1$，再交换求和号。

15.

y	3	5	7	11
$\Phi(400,y)$	132	105	90	81
$400\prod_{p\le y}\left(1-\frac{1}{p}\right)\approx$	133	106	91	83

y	5	7	11	17	29
$\Phi(1000,y)$	231	293	263	225	212
$1000\prod_{p\leqslant y}\left(1-\frac{1}{p}\right)\approx$	266	228	207	183	166

16. (ii)

x	100	300	500	700	1000
$\pi(x;4,1)$	11	29	44	59	80
$\pi(x;4,3)$	13	32	50	65	87

习 题 二

1.

$$\pi_2(x)=\sum_{\substack{p_1p_2\leqslant x\\ p_1\leqslant p_2}}1=\sum_{p_1\leqslant\sqrt{x}}\ \sum_{p_1\leqslant p_2\leqslant x/p_1}1$$

$$=\sum_{p_1\leqslant\sqrt{x}}\{\pi(x/p_1)-\pi(p_1)+1\}。$$

再利用式(1)及(17)。

2. 当$m\geqslant 128$时，$((\ln 2)/6)m>2\ln(2m)$，由此及式(31)推出结论在$m\geqslant 128$时成立。其它直接验证。

3. 由式(31)知，当$m\geqslant 128$时，$\pi(2m)-\pi(m)>c_1m/\ln(2m)$，这就可推出所要结论，$c_1=(\ln 2)/6$。

4. (i) $\psi(x)=\sum_{p^k\leqslant x}\Lambda(p^k)=\sum_{k=1}^{\infty}\sum_{p\leqslant x^{1/k}}\ln p$。

(ii) $\theta(x)=\sum_{n=1}^{\infty}\psi(x^{1/n})\sum_{d\mid n}\mu(d)$，交换求和号，由(i)即得。

5．在证明式(33)时，得到 $\psi(x)\leqslant\theta(x)+\ln x\cdot\sum\limits_{p\leqslant\sqrt{x}}1$．由此及式(1)即得所要结论。

6．由式(2)可得 $\lim\limits_{n\to\infty}\ln p_n/\ln n=1$。若 $\lim\limits_{x\to\infty}\pi(x)(\ln x)/x=1$，取 $x=p_n$ 就推出 $\lim\limits_{n\to\infty}p_n/(n\ln n)=1$，若后一极限成立，则必有 $p_n\leqslant x<p_{n+1}$，因而 $(n\ln p_n)/p_{n+1}<\pi(x)(\ln x)/x<(n\ln p_{n+1})/p_n$，由此推出前一极限成立。

7．$\psi(x)=\sum\limits_{m\leqslant x}\psi(x/m)\sum\limits_{d\mid m}\mu(d)$，交换求和号，利用式(39)即得所要结论。

8．(i) 利用式(16)；(ii) 利用式(39)；(iii) 由(ii)推出；(iv) 利用 $\psi(x)=\sum\limits_{n=0}^{\infty}\{\psi(x/6^n)-\psi(x/6^{n+1})\}$，由(i)，(iii) 推出．

9．(i) 由式 (39) 和(41) 可得 $\ln([x]!)=x\sum\limits_{k\leqslant x}\Lambda(k)/k-\sum\limits_{k\leqslant x}\Lambda(k)\{x/k\}$。由此利用式(16)和(44)即得所要结果；(ii) 由(i)推出。

10．$\int_a^b f(t)dt=\left(\int_a^{[a]+1}+\int_{[a]+1}^{[a]+2}+\cdots+\int_{[b]-1}^{[b]}+\int_{[b]}^{b}\right)f(t)dt$．

11．同上题。

13．利用式(17)及级数收敛判别法。

14．利用式(38)。

习 题 三

1．(i) 由有限个绝对收敛级数相乘可以任意聚项、算术基本定理、及条件知

$$\left|\prod_{p\leqslant x}(1+f(p)p^{-s}+f(p^2)p^{-2s}+\cdots)-\sum_{n\leqslant x}f(n)n^{-s}\right|$$

$$\leqslant \sum_{n>x} |f(n)| n^{-s}.$$

由此即得所要结论；(ii) 由(i)推出。

2. 绝对收敛级数相乘，可以任意紧项。

3. (i) 由第 1 题(i)推出；(ii) 由(i)及式(9)推出；(iii) $1=\zeta(s)\sum_{n=1}^{\infty}\mu(n)n^{-s}, s>1$，再利用第 2 题，然后比较两边系数。

4. 利用第 1 题及式(9)。

5. (i) 由第 1 题(ii)及上题推出；(ii) $\zeta(s)\sum_{n=1}^{\infty}\lambda(n)n^{-s}=\zeta(2s), s>1$，利用第 2 题，再比较两边系数；(iii) 利用第 4 题、第 2 题，用同上的方法证。

6. 利用第 1 题(i)，或第 2 题均可证明。

7. 利用第 1 题(i)，及

$$1+(p-1)p^{-s}+p(p-1)p^{-2s}+\cdots+p^{m}(p-1)p^{-(m+1)s}+\cdots$$
$$=1+(p-1)p^{-s}/(1-p^{-s+1})=(1-p^{-s})/(1-p^{-s+1}).$$

由这一证明，利用第 2 题就可给出两个关系式的新证明。

8. (i) 对 $\ln\zeta(s)=-\sum_{p}\ln(1-p^{-s})$ 两边求导即得；

(ii) 利用第 2 题。

第 九 章

习 题 一

1. 根据定义证。

2. 利用算术基本定理。

3. $(f(-1))^2=f((-1)\cdot(-1))=f(1)=1$.

4. 设 $(n_1,n_2)=1, n=n_1n_2$. 那么，$n=m^k \Longleftrightarrow n_1=m_1^k, n_2=m_2^k$。所以 $P_k(n)$ 是积性的。$k=1$ 时，显见 $P_1(n)\equiv 1$ 是完全积性的；若 $P_k(n)$ 是完全积性的，则必有 $k=1$，如不然，$k>1$，则有

$1 = P_k(2^k) = P_k(2)P_k(2)\cdots P_k(2) = 0$，矛盾。若 $n = m^k$，则 $(m-1)^k \leqslant n-1 < m^k$；若 $(m-1)^k < n < m^k$，则 $(m-1)^k \leqslant n-1 < m^k$，所以总有 $P_k(n) = [n^{1/k}] - [(n-1)^{1/k}]$。

5．设 $(n_1, n_2) = 1, n = n_1 n_2$。那么，$n$ 有大于 1 的 k 次方因数的充要条件是 n_1 或 n_2 有大于 1 的 k 次方因数，所以是积性的。$k=1$ 时，显见 $Q_1(n) = [1/n]$，是完全积性的。若 $Q_k(n)$ 是完全积性的，则 $Q_k(2^k) = Q_k(2)Q_k(2^{k-1}) = 1$，所以必有 $k=1$。

6．设 $(n_1, n_2) = 1, n = n_1 n_2$。那么，$n = d_1 \cdots d_l$ 的充要条件是 $n_1 = d_{11} \cdots d_{l1}, n_2 = d_{12} \cdots d_{l2}, d_{j1} = (d_j, n_1)$，$d_{j2} = (d_j, n_2)$。由此就推出 $\tau_l(n)$ 是积性，$\tau_l(p^\alpha)(l \geqslant 2)$ 等于不定方程 $x_1 + \cdots + x_l = \alpha$，$x_j \geqslant 0$ 的解数，即 $(\alpha + l - 1)!/(\alpha!(l-1)!)$。

7．类似上题证明积性。$\tau_1^*(n) \equiv 1$。$\tau_l^*(p^\alpha)(l \geqslant 2)$ 等于不定方程 $x_1 + \cdots + x_l = \alpha, x_j \geqslant 0$ 且不能同时有两个 $\geqslant 1$，因此等于 l。$\tau_l^*(n) = l^{\omega(n)}$。

8．$T(p^\alpha) = 2, T(n) = 2^{\omega(n)}$。

习　题　二

1．(i) 两边都是积性函数，利用 § 1定理 1 证；

(ii) 由定义推出。

2．是积性函数，当 $n = p^\alpha$ 时等于 2，对其它的 $n > 1$，等于零。

3．是积性函数，设 K 的不同的素因数为 $p_1, \cdots, p_r$。当 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 时，等于 $2^{\Omega(n)}$，对其它的 $n > 1$ 等于零。

4．这不是积性函数，直接用定理 1(i) 计算，$n=1$ 时等于零；当 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 时，等于

$$\sum_{\substack{k_1 + \cdots + k_r = m \\ k_j \geqslant 1}} (-1)^r \frac{m!}{k_1! \cdots k_r!} \ln^{k_1} p_1 \cdots \ln^{k_r} p_r.$$

当 $r > m$ 时，$k_1 + \cdots + k_r = m, k_j \geqslant 1$ 无解，故必为零。

5．$F_1(n) = \sum_{d \mid n} f(d)$，$F_2(m) = \sum_{n \mid m} F_1(n) = \sum_{n \mid m} \sum_{d \mid n} f(d)$，交

换求和号。

6．表 $n=m^k n_1$，n_1 无大于 1 的 k 次方因数。

$$\sum_{d^k\mid n} f(d^l)=\sum_{d\mid m} f(d^l).$$

7．直接验证，利用上题。

8．$\sum\limits_{d\mid n}|\mu(n)|=2^{\omega(n)}$，$\sum\limits_{d\mid n}\mu(d)|\mu(n/d)|=1$，当 $n=1$；$=0$，当 $n=p$ 或 p^a，$a>2$；$=-1$，当 $n=p^2$，即

$$\sum_{d\mid n}\mu(d)|\mu(n/d)|=\begin{cases}1, & n=1,\\ (-1)^r, & n=p_1^2\cdots p_r^2,\\ 0, & \text{其它}.\end{cases}$$

9．设 $n=p_1^{a_1}\cdots p_r^{a_r}$。$\sum\limits_{d\mid n}P_k(d)=\prod\limits_{i=1}^{r}(1+[a_i/k])$。再设 $\rho(r)=1$，$r=0$；$\rho(r)=-1$，$r=1$，及 $\rho(r)=0$，$r\geqslant 2$。

$$\sum_{d\mid n}\mu(n/d)P_k(d)=\prod_{i=1}^{r}\rho(a_i-[a_i/k]\cdot k).$$

当 $k=2$ 时，$a-2[a/2]=0$，$2\mid a$；1，$2\nmid a$。由此就推出这时的 Möbius 逆变换是 $\lambda(n)=(-1)^{\Omega(n)}$。

10．设 $n=p_1^{a_1}\cdots p_r^{a_r}$。$\sum\limits_{d\mid n}Q_k(d)=\prod\limits_{i=1}^{r}(1+\min(a_i,k-1))$。

$$\begin{aligned}\sum_{d\mid n}\mu(n/d)Q_k(d)&=\prod_{i=1}^{r}(Q_k(p^a)-Q_k(p^{a-1}))\\&=\begin{cases}(-1)^r, & \text{当 } a_1=\cdots=a_r=k;\\ 0, & \text{其它的 } n>1.\end{cases}\end{aligned}$$

11．设 $n_1^{-1}n_1\equiv 1(\bmod n_2)$，$n_2^{-1}n_2\equiv 1(\bmod n_1)$，$n=n_1n_2$，$(n_1,n_2)=1$。因孙子定理知：$d=n_2^{-1}n_2d_1+n_1^{-1}n_1d_2$，$d$ 遍历模 n 的完全剩余系的充要条件是 d_1，d_2 分别遍历模 n_1，n_2 的完全剩余系。$(d,n)=1$ 的充要条件是 $(d_1,n_1)=(d_2,n_2)=1$，$(d+1,n)=1$ 的充要条件

是$(d_1+1,n_1)=(d_2+1,n_2)=1$。这就证明了 $f(n)$ 是积性的。显见 $f(p^\alpha)=p^\alpha(1-2/p)$。

12. (i) $\phi_k(n)=\sum_{1\leq d_1\leq n}\cdots\sum_{1\leq d_k\leq n}\sum_{d\mid(d_1,\cdots,d_k,n)}\mu(d)$

$=\sum_{d\mid n}\mu(d)(n/d)^k$。另一证法是

$$\sum_{d\mid n}\phi_k(d)=\sum_{d\mid n}\sum_{\substack{(d_1,\cdots,d_k,d)=1\\ 1\leq d_j\leq d}}1$$

$$=\sum_{d\mid n}\sum_{1\leq d_1,\cdots,d_k\leq d}\sum_{l\mid(d_1,\cdots,d_k,d)}\mu(l)$$

$$=\sum_{l\mid n}\mu(l)\sum_{l\mid d\mid n}\sum_{\substack{1\leq d_1,\cdots,d_k\leq d\\ l\mid d_1,\cdots,d_j}}1=\sum_{l\mid n}\mu(l)\sum_{h\mid n/l}h^k$$

$$=\sum_{h\mid n}h^k\sum_{l\mid n/h}\mu(l)=n^k。$$

(ii) 由 $\phi_k(n)$的积性推出。

13. (i) 利用上题方法，由 $S_k(n)=n^{-k}\sum_{d\mid n}\sum_{\substack{j=1\\(j,n)=d}}j^k$，或

$\sum_{d\mid n}S_k^*(d)=\sum_{d\mid n}d^{-k}\sum_{j=1}^{d}j^2\left(\sum_{l\mid(d,j)}\mu(l)\right)$，即可推出；

(ii) 当 $n>1$ 时，

$$S_1^*(n)=\sum_{d\mid n}\mu(d)S_1(n/d)$$

$$=\sum_{d\mid n}\mu(d)(1/2+n/(2d))=\phi(n)/2;$$

$$S_2^*(n)=\sum_{d\mid n}\mu(d)S_2(n/d)$$

$$= \sum_{d|n} \mu(d)(1/2 + n/(3d) + d/(6n))$$

$$= \phi(n)/3 + (1/6n)\prod_{p|n}(1-p).$$

15. 和定理 4，定理 5 的论证相同。

17. 无论按怎样的次序作卷积 $f_1 * f_2 * \cdots * f_r$，必有

$$(f_1 * \cdots * f_r)(n) = \sum_{d_1 \cdots d_r = n} f_1(d_1) \cdots f_r(d_r).$$

18. (i) 利用定理 1(ii)的第二个证明方法，即利用引理 2；(ii) 利用定理 6 的第一个证明方法。

19. 直接验证，或利用第18题验证，或利用卷积性质推导。例如：由(i)—(iv)可推出 $\sigma = U * E = U * (U * \phi) = \tau * \phi$，即(v)成立。

21. 利用归纳法证存在性及唯一性。

22. 利用第18题(ii)。

23. (i)，(ii)由第19题(i)，(ii)推出；(iii) $E^{-1}(1) = 1$，$E^{-1}(p) = -p, E^{-1}(p^\alpha) = 0, \alpha \geqslant 2$，即$E^{-1} = \mu E$；(iv) $\sigma^{-1} = \mu * E^{-1}$，$\sigma^{-1}(p^\alpha) = E^{-1}(p^\alpha) - E^{-1}(p^{\alpha-1}) = -p-1, \alpha = 1$；$p, \alpha = 2$；$0, \alpha > 2$。$\phi^{-1} = U * E^{-1}, \phi^{-1}(p^\alpha) = 1 - p, \alpha \geqslant 1$；(v) $\lambda^{-1} = \mu^2$。

24. (i) $n = 1$ 显然成立，当 $n = p$ 时，由定义知 $f^{-1}(p) = -f(p)$，所以结论成立；(ii) 由定义及(i)推出

25. 由上题(ii)，利用归纳法推出必要性。充分性亦由上题(i)和(ii)，利用归纳法推出。

26. (i) 直接验证$(fg^{-1}) * (fg)^{-1} = I$；(ii) 在(i)中取 $g = U$。

27. 必要性即上题(ii)，充分性同第25题的充分性。

28. 直接验证。$(\mu^2 \times E)(p^\alpha) = \sum_{d|p^\alpha} \mu^2(d)(p^\alpha/d) = p^\alpha + p^{\alpha-1}$。

$$\sum_{d^2|p^\alpha} \mu(d)\sigma(p^\alpha/d^2) = \begin{cases} \sigma(p) = p+1, & \text{当}\alpha = 1; \\ \sigma(p^\alpha) - \sigma(p^{\alpha-2}) \\ \quad = p^\alpha + p^{\alpha-1}, & \text{当}\alpha \geqslant 2. \end{cases}$$

习 题 三

1. 由式(14)知，只要证明：

$$I = \int_1^{\infty}\{(t-[t])/t[t]+(t-[t])/t^2\}dt = 1.$$

$$I = \sum_{n=1}^{\infty}\int_n^{n+1}(1/n - n/t^2)dt = \sum_{n=1}(1/n - 1/(n+1)) = 1.$$

也可利用引理10来证，取 $b(n)\equiv 1$，$a(x)=1/x, x_1=1$。

2. 用引理 2 的证法证，或用引理10证。

3. $\sum_{n\leqslant x}\sigma(n) = \sum_{kl\leqslant x}k$，再利用式(23)计算。

4. $\sum_{n\leqslant x}\mu^2(n) = \sum_{d\leqslant\sqrt{x}}\mu(d)\left[\frac{x}{d^2}\right]$。

5. $$2^{\omega(n)} = \sum_{\substack{n=d_1d_2\\(d_1,d_2)=1}}1 = \sum_{n=d_1d_2}\sum_{l\mid(d_1,d_2)}\mu(l).$$

$$\sum_{n\leqslant x}2^{\omega(n)} = \sum_{l\leqslant\sqrt{x}}\mu(l)\sum_{k_1k_2\leqslant x/l^2}1$$

$$= \sum_{l\leqslant\sqrt{x}}\mu(l)D(x/l^2).$$

6. 利用上题及定理 3 .

7. 可直接求渐近公式，也可以利用引理10及相应的渐近公式推出。

8. (i) 利用式(30)的下面一式及式(36)；

(ii) 由 $\varphi(n) = n\sum_{d\mid n}\mu(d)/d$ 立即推出。

9．(i) $\sigma(n)=\prod_{p\mid n}(p^{\alpha+1}-1)/(p-1)$，$\frac{n^2}{\phi(n)}=n\prod_{p\mid n}\frac{p}{p-1}$.

所以

$$n^2/(\sigma(n)\phi(n))=\prod_{p\mid n}(1-1/p^{\alpha+1});$$

(ii) 由(i) 及第 7 题(ii)推出；

(iii) 由(i)及第 7 题(ii)推出。

10．$\sum_{n\leqslant x}\phi_1(x)=\sum_{d\leqslant\sqrt{x}}\mu(d)\sum_{k\leqslant x/d^2}\sigma(k)$，再利用第 3 题。

12．利用第11题。

13．利用第11题。

14．这时，上题中的$F(s)=\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$，由此即得所要結论。也可直接利用第11题证。

15．$\sum_{n\leqslant x}\sigma_t(n)=\sum_{k\leqslant x}\sum_{d\leqslant x/k}d^t$，再利用第12题和第13题。

16．$\sum_{n\leqslant x}\sigma_{-t}(n)=\sum_{d\leqslant x}d^{-t}[x/d]$，再利用第13题。

17．利用$\frac{1}{p}<\ln\left(1-\frac{1}{p}\right)^{-1}<\frac{1}{p-1}=\frac{1}{p}+\frac{1}{(p-1)p}$，由定理11推出。

18．利用定理11和引理10。

19．利用定理11和引理10。

20．$\sum_{pq\leqslant x}\frac{1}{pq}=\sum_{p\leqslant x/2}\frac{1}{p}\sum_{q\leqslant x/p}\frac{1}{q}$，先利用定理 11，再利用定理 9 估计次要项。

21．(i) $\sum_{n\leqslant x}\omega(n)=\sum_{n\leqslant x}\sum_{p\mid n}1=\sum_{p\leqslant x}[x/p]$，再利用定理11；

(ii) $\sum_{n\leqslant x}\Omega(n)-\sum_{n\leqslant x}\omega(n)=\sum_{n\leqslant x}\sum_{p^k\mid n,\,k>1}1=\sum_{k>1,\,p^k\leqslant x}[x/p^k]$

$$=\sum_{k>1,\ p^k\le x} x/p^k+r_1(x)=x\sum_{p\le x}\sum_{k=2}^{\infty}1/p^k-x\sum_{p\le x}\sum_{\substack{k\\ p^k>x}}1/p^k+r_1(x)$$

$=x\sum\limits_{p\le x}1/(p(p-1))+r_2(x)+r_1(x)$，这里$|r_1(x)|\leqslant A_1x^{1/2}$，$|r_2(x)|\leqslant A_2\pi(x)$，$A_1,A_2$是两个绝对正常数。由此及(i)即得(ii)。

22．设p,q是素变数。

$$\sum_{n\le x}\omega^2(n)=\sum_{n\le x}\Big(\sum_{p\mid n}1\Big)\Big(\sum_{q\mid n}1\Big)=\sum_{p\le x}\sum_{q\le x}\sum_{p\mid n,\,q\mid n,\,n\le x}1$$

$$=\sum_{p=q}+\sum_{p\ne q}=S_1+S_2.$$

显见$S_1=\sum\limits_{n\le x}\omega(n)$。只要估计$S_2$。

$$S_2=\sum_{\substack{pq\le x\\ p\ne q}}[x/(pq)]=\sum_{\substack{pq\le x\\ p\ne q}}x/(pq)+r_1(x)$$

$$=x\sum_{pq\le x}1/pq+r_1(x)+r_2(x),$$

这里$|r_1(x)|\leqslant\pi_2(x)$，$\pi_2(x)$由第八章习题二第2题给出．$|r_2(x)|\leqslant Ax$，$A$为一绝对正常数。再利用第20题，第21题(i)即可推出所要结果。

习 题 四

1．模6的特征有两个：一个是主特征$\chi(n;6,0)$，一个是非主实特征：$\chi(n;6,1)=1,n\equiv1(\mathrm{mod}\ 6)$；$=-1,n\equiv-1(\mathrm{mod}\ 6)$。模7的特征有六个：一个是主特征$\chi(n;7,0)$。其它六个是：$\chi(n;7,l)=e^{2\pi i l d/6},n\equiv3^d(\mathrm{mod}\ 7)$，$l=1,2,3,4,5,6$。$\chi(n;7,3)$是非主实特征。模8的特征有四个：$\chi(n;8,l_{-1},l_0)=e^{2\pi i l_{-1}(n-1)/2}\cdot e^{2\pi i l_0 d_0/2},n\equiv(-1)^{(n-1)/2}5^{d_0}(\mathrm{mod}\ 8)$，$l_{-1}=0,1,l_0=0,1$。除主特征$(l_{-1}=l_0=0)$外均是非主实特征。模9的特征有六个：$\chi(n;9,l)$

$=e^{2\pi i l d/6}$，$n\equiv 2^d \pmod 9$，$l=0,1,\cdots,5$，$\chi(n;9,3)$是非主实特征。模11的特征有十个：$\chi(n;11,l)=e^{2\pi i l d/10}$，$n\equiv 2^d \pmod{11}$，$l=0,1,\cdots,9$，$\chi(n;11,5)$是非主实特征。模13的特征有十二个：$\chi(n;13,l)=e^{2\pi i l d/12}$，$n\equiv 2^d \pmod{13}$，$l=0,1,\cdots,11$，$\chi(n;13,6)$是非主实特征。模15的特征有八个：$\chi(n;15,l_1,l_2)=e^{2\pi i l_1 d_1/2}\cdot e^{2\pi i l_2 d_2/4}$，$n\equiv 2^{d_1} \pmod 3$，$n\equiv 2^{d_2} \pmod 5$，$l_1=0,1$，$l_2=0,1,2,3$。非主实特征有三个：$\chi(n;15,0,2)$，$\chi(n;15,1,0)$，$\chi(n;15,1,2)$。模20的特征有八个：$\chi(n;20,l_{-1},l_1)=(-1)^{l_0(n-1)/2}e^{2\pi i l_1 d_1/4}$，$n\equiv 2^{d_1} \pmod 5$，$l_0=0,1$，$l_1=0,1,\cdots,3$，非主实特征有三个：$\chi(n;20,0,2)$，$\chi(n;20,1,0)$，$\chi(n;20,1,2)$。

3．利用表示式(33)．模 p^a 的主特征 $\chi(n;p^a,0)=\chi(n;p,0)$，模 p^a 的非主实特征 $\chi(n;p^a,\phi(p^a)/2)=\chi(n;p,(p-1)/2)=\left(\frac{n}{p}\right)$，这里用表示式(28)，对给定的 p，所有模 $p^a(a\geqslant 1)$ 取同样的原根。模 2 的实特征由取 $\beta_{-1}=\beta_0=2$ 给出，模 4 的实特征由取 $\beta_0=2,\beta_{-1}=1,2$ 给出（直接验证，及见式(9)后的说明）。模 $2^{a_0}(a_0\geqslant 3)$ 的实特征，由式(32)知是：$\chi(n;2^{a_0},l_{-1},0)=\chi(n;8,l_{-1},0)=\chi(n;4,l_{-1})$，即取 $\beta_{-1}=1,2,\beta_0=0$；$\chi(n;2^{a_0},l_{-1},2^{a_0-3})=\chi(n;8,l_{-1},1)=\chi(n;4,l_{-1})\cdot\chi(n;8,0,1)=\chi(n;4,l_{-1})\left(\frac{2}{n}\right)=\chi(n;4;l_{-1})\left(\frac{8}{n}\right)$，即取 $\beta_{-1}=1,2,\beta_0=1$。

4．(i) 用带余数除法，(ii) 只要证当 $(n,q_0)>1$ 时 $f(n)=0$。也就是要证对任一 $p|q_0$ 必有 $f(p)=0$。若 $f(p)\neq 0$，设 $p^a\|q_0$，$q_0=p^aq_1$。$f(p^a)\cdot f(n+q_1)=f(p^an+q_0)=f(p^an)=f(p^a)f(n)$，因此，$f(n+q_1)=f(n)$，即 q_1 也是周期，和 q_0 的最小性矛盾。

5．当 $\mu(k)\neq 0$ 时，对任意的 $k>q|k$，模 k 的特征一定不是模 q 的特征。再利用上题(ii)。

6．(i) $p^a/(l,p^{a-1})$；(ii) $2^a/((l_{-1},2)\cdot(l_0,2^{a-3}))$；(iii) 设 $\chi(n;k)$ 的最小正周期为 q，$\chi(n;2^{a_0})$，$\chi(n;p_1^{a_1})$，$\cdots$，$\chi(n;p_s^{a_s})$ 的最

小正周期分别为$q_0,q_1,\cdots,q_s$。显见$q|q_0q_1\cdots q_s$。设$P=p_0^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$P=p_j^{\alpha_j}P_j$，$j=0,1,\cdots,s$，这里取$p_0=2$。我们来证必有$q_j|q$，$0\leqslant j\leqslant s$。由于$q_j|p_j^{\alpha_j}$，所以$q_j$两两既约，由此就推出$q_0q_1\cdots q_s|q$。以$q_0|q$为例来证。设$n\equiv m(\bmod 2^{\alpha_0})$，$n\equiv 1(\bmod p_j^{\alpha_j})$，$1\leqslant j\leqslant s$，$m$为任意整数。我们有$\chi(m;2^{\alpha_0})=\chi(n;k)=\chi(n+qP_0;k)=\chi(m+qP_0;2^{\alpha_0})$，因此，$q_0|qP_0$，由此及$(q_0,P_0)=1$推出$q_0|q$。其它类似证明。

7. (i) 用带余数除法；(ii) $(n_1n_2,k)=1$，$n_1\equiv n_2(\bmod k')$等价于$(n_1n_2,k)=1$，$n_1n_2^{-1}\equiv 1(\bmod k')$。

8. (i),(ii),(iii)直接验证；(iv),(v)利用相应的表示式(28),(32)，上题的(i)，对给定的原根g(当$k=p^{\alpha}$，p奇素数，所有的$\alpha\geqslant 1$)，n对模p^{α_1}的指标与对模p^{α_2}的指标之间的关系($\alpha_1>\alpha_2$)，以及对$-1,5$，n对模2^{α_1}的指标组与对模2^{α_2}的指标组之间的关系($\alpha_1>\alpha_2$)；(vi) 利用定义及孙子定理。

9. (i) 利用上题(vi)；

(ii) 设k是给定的正整数。对模k的每个特征$\chi(n;k)$必唯一的对应一个模$d|k$及模d的一个原特征$\chi^*(n;d)$，且反过来也对(即第12题)。由此及模k有$\phi(k)$个特征即推出所要结论；

(iii) $P(k)=\sum\limits_{d|k}\mu(d)\phi(k/d)$。$P(p^{\alpha})=p-2$，当$\alpha=1$；$=p^{\alpha}-2p^{\alpha-1}+p^{\alpha-2}$，当$\alpha>1$。

10. 利用第3题及第8题的(iv),(v)。

11. 由特征的表示式及第8题的(iv)和(v)，即可推出。

12. 利用上题及第8题(vi)。也容易直接证，但要用原特征的定义。

13. $\chi(n;p^{\alpha})$为非主特征时，对应的$k^*=p^{\lambda}\neq 1$，$\lambda\leqslant\alpha$。这时$(n,p^{\alpha})=1$与$(n,p)=1$是一样的。只要在表示式(24)右边出现一个主特征时，就不成立。

14. 由表示式(24),(28)及(32)推出。

15．直接验证。这是周期数论函数的有限 Fourier 展开。

16．(vi) 利用剩余系的分解；(vii) 即第八章习题一第 13 题，一般情形类似证明。

17．(iii) 必有$(m,k)=1$, $m\equiv1(\bmod k')$使 $\chi(m)\neq1$（见第 7 题(ii)），证明 $\chi(m)S(n)=S(n)$。

18．(i)由上题(iv)及第16题(v)推出；(ii)考虑$\sum_{a=1}^{k}|G(a;\chi)|^2$，利用(i)及式(58)两种方法来计算这和式，比较即得；(iii) 利用第16题(iii)，由此亦推出(iv)。

19．由第16题(vi)知只要讨论 $k=p^a$ 的情形。利用第13题直接计算。

20．$\sum_{n=M+1}^{M+N}\chi(n)=(G(1;\bar{\chi}))^{-1}\sum_{n=M+1}^{M+N}G(n;\bar{\chi})$（这里利用了第18题）。再代入式(58)直接计算即得第一个不等式。再利用当$0\leqslant x\leqslant\pi/2$ 时，$2x/\pi\leqslant\sin x$，分 k 为奇、偶数两种情形来估计第一个不等式的右边部分，即得第二个不等式。

21．$\sum_{n=M+1}^{M+N}\chi(n)=\sum_{\substack{n=M+1\\(n,k_2)=1}}^{N+M}\chi^*(n;k^*)$。这里 $k=k_1k_2$，k_1 和 k^* 有相同的素因数，$k^*|k_1$，$(k_1,k_2)=1$。再利用$\sum_{d|n}\mu(d)=[1/n]$及上题估计。

22．利用式(48)及第20题。

23．(iii) 设不超过 x 的正的模 p 的二次剩余个数为 $R(x)$。

$$R(x)-N(x)=\sum_{a=1}^{[x]}\left(\frac{a}{p}\right)=\theta\sqrt{p}\ln p,\ |\theta|\leqslant1$$

（这由第20题推出）。此外显然有 $R(x)+N(x)=[x]$。

24．(i) 第一部分利用第21题，第二部分是第八章习题三第 1 题(ii)的特例；

(ii) 类似第八章习题三第 3 题证明；

(iii) 利用(i)；(iv) 利用(i)或(iii)均可。

25．(i) 利用定理 7；(ii) 由(i)推出。

26．同余方程 $f(x_1,\cdots,x_r)\equiv 0\pmod p$，$1\leqslant x_j\leqslant a_j$，$1\leqslant j\leqslant r$ 的解的个数为 $p^{-1}\sum_{x_1=1}^{a_1}\cdots\sum_{x_r=1}^{a_r}\sum_{l=1}^{p}e^{2\pi i l f(x_1,\cdots,x_r)/p}$。由此利用容斥原理就可推出(ii)及(iii)中的公式。(i)，(ii)，(iii)中的具体结果容易直接证明；

(iv)

$$T_p^*(3)=(48)^{-1}(p-1)\left(p-8-(-1)^{(p-1)/2}3\left(1+2\left(\frac{2}{p}\right)\right)\right),$$

$$T_p^*(4)=(3\cdot 2^7)^{-1}(p-1)\Bigg(p^2-14p+\Bigg(71+(-1)^{(p-1)/2}30$$
$$+24(-1)^{(p-1)/2}\left(\frac{2}{p}\right)+32(-1)^{(p-1)/2}\left(\frac{3}{p}\right)\Bigg)\Bigg).$$

附表1　素数与最小正原根表(5000以内)①

(加*者表示10为其原根)

p	$p-1$	g	p	$p-1$	g
3	2	2	127	$2\cdot3^2\cdot7$	3
5	2^2	2	131*	$2\cdot5\cdot13$	2
7*	$2\cdot3$	3	137	$2^3\cdot17$	3
11	$2\cdot5$	2	139	$2\cdot3\cdot23$	2
13	$2^2\cdot3$	2	149*	$2^2\cdot37$	2
17*	2^4	3	151	$2\cdot3\cdot5^2$	6
19*	$2\cdot3^2$	2	157	$2^2\cdot3\cdot13$	5
23*	$2\cdot11$	5	163	$2\cdot3^4$	2
29*	$2^2\cdot7$	2	167*	$2\cdot83$	5
31	$2\cdot3\cdot5$	3	173	$2^2\cdot43$	2
37	$2^2\cdot3^2$	2	179*	$2\cdot89$	2
41	$2^3\cdot5$	6	181*	$2^2\cdot3^2\cdot5$	2
43	$2\cdot3\cdot7$	3	191	$2\cdot5\cdot19$	19
47*	$2\cdot23$	5	193*	$2^6\cdot3$	5
53	$2^2\cdot13$	2	197	$2^2\cdot7^2$	2
59*	$2\cdot29$	2	199	$2\cdot3^2\cdot11$	3
61*	$2^2\cdot3\cdot5$	2	211	$2\cdot3\cdot5\cdot7$	2
67	$2\cdot3\cdot11$	2	223*	$2\cdot3\cdot37$	3
71	$2\cdot5\cdot7$	7	227	$2\cdot113$	2
73	$2^3\cdot3^2$	5	229*	$2^2\cdot3\cdot19$	6
79	$2\cdot3\cdot13$	3	233*	$2^3\cdot29$	3
83	$2\cdot41$	2	239	$2\cdot7\cdot17$	7
89	$2^3\cdot11$	3	241	$2^4\cdot3\cdot5$	7
97*	$2^5\cdot3$	5	251	$2\cdot5^3$	6
101	$2^2\cdot5^2$	2	257*	2^8	3
103	$2\cdot3\cdot17$	5	263*	$2\cdot131$	5
107	$2\cdot53$	2	269*	$2^2\cdot67$	2
109*	$2^2\cdot3^3$	6	271	$2\cdot3^3\cdot5$	6
113*	$2^4\cdot7$	3	277	$2^2\cdot3\cdot23$	5

① 本表取自参考书[2]。原表1459,3631,4111三个素数的最小正原根有误。参看胸大正，从计算看素数的最小原根，数学的实践与认识，1992，第3期。

续

p	$p-1$	g	p	$p-1$	g
281	$2^3\cdot5\cdot7$	3	487*	$2\cdot3^5$	3
283	$2\cdot3\cdot47$	3	491*	$2\cdot5\cdot7^2$	2
293	$2^2\cdot73$	2	499*	$2\cdot3\cdot83$	7
307	$2\cdot3^2\cdot17$	5	503*	$2\cdot251$	5
311	$2\cdot5\cdot31$	17	509*	$2^2\cdot127$	2
313*	$2^3\cdot3\cdot13$	10	521	$2^3\cdot5\cdot13$	3
317	$2^2\cdot79$	2	523	$2\cdot3^2\cdot29$	2
331	$2\cdot3\cdot5\cdot11$	3	541*	$2^2\cdot3^3\cdot5$	2
337*	$2^4\cdot3\cdot7$	10	547	$2\cdot3\cdot7\cdot13$	2
347	$2\cdot173$	2	557	$2^2\cdot139$	2
349	$2^2\cdot3\cdot29$	2	563	$2\cdot281$	2
353	$2^5\cdot11$	3	569	$2^3\cdot71$	3
359	$2\cdot179$	7	571*	$2\cdot3\cdot5\cdot19$	3
367*	$2\cdot3\cdot61$	6	577*	$2^6\cdot3^2$	5
373	$2^2\cdot3\cdot31$	2	587	$2\cdot293$	2
379*	$2\cdot3^3\cdot7$	2	593*	$2^4\cdot37$	3
383*	$2\cdot191$	5	599	$2\cdot13\cdot23$	7
389*	$2^2\cdot97$	2	601	$2^3\cdot3\cdot5^2$	7
397	$2^2\cdot3^2\cdot11$	5	607	$2\cdot3\cdot101$	3
401	$2^4\cdot5^2$	3	613	$2^2\cdot3^2\cdot17$	2
409	$2^3\cdot3\cdot17$	21	617	$2^3\cdot7\cdot11$	3
419*	$2\cdot11\cdot19$	2	619*	$2\cdot3\cdot103$	2
421	$2^2\cdot3\cdot5\cdot7$	2	631	$2\cdot3^2\cdot5\cdot7$	3
431	$2\cdot5\cdot43$	7	641	$2^7\cdot5$	3
433*	$2^4\cdot3^3$	5	643	$2\cdot3\cdot107$	11
439	$2\cdot3\cdot73$	15	647*	$2\cdot17\cdot19$	5
443	$2\cdot13\cdot17$	2	653	$2^2\cdot163$	2
449	$2^6\cdot7$	3	659*	$2\cdot7\cdot47$	2
457	$2^3\cdot3\cdot19$	13	661	$2^2\cdot3\cdot5\cdot11$	2
461*	$2^2\cdot5\cdot23$	2	673	$2^5\cdot3\cdot7$	5
463	$2\cdot3\cdot7\cdot11$	3	677	$2^2\cdot13^2$	2
467	$2\cdot233$	2	683	$2\cdot11\cdot31$	5
479	$2\cdot239$	13	691	$2\cdot3\cdot5\cdot23$	3

续

p	$p-1$	g	p	$p-1$	g
701*	$2^2\cdot5^2\cdot7$	2	937*	$2^3\cdot3^2\cdot13$	5
709*	$2^2\cdot3\cdot59$	2	941*	$2^2\cdot5\cdot47$	2
719	$2\cdot359$	11	947	$2\cdot11\cdot43$	2
727*	$2\cdot3\cdot11^2$	5	953*	$2^3\cdot7\cdot17$	3
733	$2^2\cdot3\cdot61$	6	967	$2\cdot3\cdot7\cdot23$	5
739	$2\cdot3^2\cdot41$	3	971*	$2\cdot5\cdot97$	6
743*	$2\cdot7\cdot53$	5	977*	$2^4\cdot61$	3
751	$2\cdot3\cdot5$	3	983*	$2\cdot491$	5
757	$2^2\cdot3^3$	2	991	$2\cdot3^2\cdot5\cdot11$	6
761	$2^3\cdot5\cdot19$	6	997	$2^2\cdot3\cdot83$	7
769	$2^8\cdot3$	11	1009	$2^4\cdot3^2\cdot7$	11
773	$2^2\cdot193$	2	1013	$2^2\cdot11\cdot23$	3
787	$2\cdot3\cdot131$	2	1019*	$2\cdot509$	2
797	$2^2\cdot199$	2	1021*	$2^2\cdot3\cdot5\cdot17$	10
809	$2^3\cdot101$	3	1031	$2\cdot5\cdot103$	14
811*	$2\cdot3^4\cdot5$	3	1033*	$2^3\cdot3\cdot43$	5
821*	$2^2\cdot5\cdot41$	2	1039	$2\cdot3\cdot173$	3
823*	$2\cdot3\cdot137$	3	1049	$2^3\cdot131$	3
827	$2\cdot7\cdot59$	2	1051*	$2\cdot3\cdot5^2\cdot7$	7
829	$2^2\cdot3^2\cdot23$	2	1061	$2^2\cdot5\cdot53$	2
839	$2\cdot419$	11	1063*	$2\cdot3^2\cdot59$	3
853	$2^2\cdot3\cdot71$	2	1069*	$2^2\cdot3\cdot89$	6
857*	$2^3\cdot107$	3	1087*	$2\cdot3\cdot181$	3
859	$2\cdot3\cdot11\cdot13$	2	1091*	$2\cdot5\cdot109$	2
863*	$2\cdot431$	5	1093	$2^2\cdot3\cdot7\cdot13$	5
877	$2^2\cdot3\cdot73$	2	1097*	$2^3\cdot137$	3
881	$2^4\cdot5\cdot11$	3	1103*	$2\cdot19\cdot29$	5
883	$2\cdot3^2\cdot7^2$	2	1109*	$2^2\cdot277$	2
887*	$2\cdot443$	5	1117	$2^2\cdot3^2\cdot31$	2
907	$2\cdot3\cdot151$	2	1123	$2\cdot3\cdot11\cdot17$	2
911	$2\cdot5\cdot7\cdot13$	17	1129	$2^3\cdot3\cdot47$	11
919	$2\cdot3^3\cdot17$	7	1151	$2\cdot5^2\cdot23$	17
929	$2^5\cdot29$	3	1153*	$2^7\cdot3^2$	5

p	$p-1$	g	p	$p-1$	g
1163	$2\cdot7\cdot83$	5	1427	$2\cdot23\cdot31$	2
1171*	$2\cdot3^2\cdot5\cdot13$	2	1429*	$2^2\cdot3\cdot7\cdot17$	6
1181*	$2^2\cdot5\cdot59$	7	1433*	$2^3\cdot179$	3
1187	$2\cdot593$	2	1439	$2\cdot719$	7
1193*	$2^3\cdot149$	3	1447*	$2\cdot3\cdot241$	3
1201	$2^4\cdot3\cdot5^2$	11	1451	$2\cdot5^2\cdot29$	2
1213*	$2^2\cdot3\cdot101$	2	1453	$2^2\cdot3\cdot11^2$	2
1217*	$2^6\cdot19$	3	1459	$2\cdot3^6$	3
1223*	$2\cdot13\cdot47$	5	1471	$2\cdot3\cdot5\cdot7^2$	6
1229*	$2^2\cdot307$	2	1481	$2^3\cdot5\cdot37$	3
1231	$2\cdot3\cdot5\cdot41$	3	1483	$2\cdot3\cdot13\cdot19$	2
1237	$2^2\cdot3\cdot103$	2	1487*	$2\cdot743$	5
1249	$2^5\cdot3\cdot13$	7	1489	$2^4\cdot3\cdot31$	14
1259*	$2\cdot17\cdot37$	2	1493	$2^2\cdot373$	2
1277	$2^2\cdot11\cdot29$	2	1499	$2\cdot7\cdot107$	2
1279	$2\cdot3^2\cdot71$	3	1511	$2\cdot5\cdot151$	11
1283	2,641	2	1523	$2\cdot761$	2
1289	$2^3\cdot7\cdot23$	6	1531*	$2\cdot3^2\cdot5\cdot17$	2
1291*	$2\cdot3\cdot5\cdot43$	2	1543*	$2\cdot3\cdot257$	5
1297*	$2^4\cdot3^4$	10	1549*	$2^2\cdot3^2\cdot43$	2
1301*	$2^2\cdot5^2\cdot13$	2	1553*	$2^4\cdot97$	3
1303*	$2\cdot3\cdot7\cdot31$	6	1559	$2\cdot19\cdot41$	19
1307	$2\cdot653$	2	1567*	$2\cdot3^3\cdot29$	3
1319	$2\cdot659$	13	1571*	$2\cdot5\cdot157$	2
1321	$2^3\cdot3\cdot5\cdot11$	13	1579*	$2\cdot3\cdot263$	3
1327*	$2\cdot3\cdot13\cdot17$	3	1583*	$2\cdot7\cdot113$	5
1361	$2^4\cdot5\cdot17$	3	1597	$2^2\cdot3\cdot7\cdot19$	11
1367*	$2\cdot683$	5	1601	$2^6\cdot5^2$	3
1373	$2^2\cdot7^3$	2	1607*	$2\cdot11\cdot73$	5
1381*	$2^2\cdot3\cdot5\cdot23$	2	1609	$2^3\cdot3\cdot67$	7
1399	$2\cdot3\cdot233$	13	1613	$2^2\cdot13\cdot31$	3
1409	$2^7\cdot11$	3	1619*	$2\cdot809$	2
1423	$2\cdot3^2\cdot79$	3	1621*	$2^2\cdot3^4\cdot5$	2

p	$p-1$	g	p	$p-1$	g
1627	$2\cdot3\cdot271$	3	1901	$2^2\cdot3^2\cdot19$	2
1637	$2^2\cdot409$	2	1907	$2\cdot953$	2
1657	$2^3\cdot3^2\cdot23$	11	1913*	$2^3\cdot239$	3
1663*	$2\cdot3\cdot277$	3	1931	$2\cdot5\cdot193$	2
1667	$2\cdot7^2\cdot17$	2	1933	$2^2\cdot3\cdot7\cdot23$	5
1669	$2^2\cdot3\cdot139$	2	1949*	$2^2\cdot487$	2
1693	$2^2\cdot3^2\cdot47$	2	1951	$2\cdot3\cdot5^2\cdot13$	3
1697*	$2^5\cdot53$	3	1973	$2^2\cdot17\cdot29$	2
1699	$2\cdot3\cdot283$	3	1979*	$2\cdot23\cdot43$	2
1709*	$2^2\cdot7\cdot61$	3	1987	$2\cdot3\cdot331$	2
1721	$2^3\cdot5\cdot43$	3	1993*	$2^3\cdot3\cdot83$	5
1723	$2\cdot3\cdot7\cdot41$	3	1997	$2^2\cdot499$	2
1733	$2^2\cdot433$	2	1999	$2\cdot3^3\cdot37$	3
1741*	$2^2\cdot3\cdot5\cdot29$	2	2003	$2\cdot7\cdot11\cdot13$	5
1747	$2\cdot3^2\cdot97$	2	2011	$2\cdot3\cdot5\cdot67$	3
1753	$2^3\cdot3\cdot73$	7	2017*	$2^5\cdot3^2\cdot7$	5
1759	$2\cdot3\cdot293$	6	2027	$2\cdot1013$	2
1777*	$2^4\cdot3\cdot37$	5	2029*	$2^2\cdot3\cdot13^2$	2
1783*	$2\cdot3^4\cdot11$	10	2039	$2\cdot1019$	7
1787	$2\cdot19\cdot47$	2	2053	$2^2\cdot3^3\cdot19$	2
1789*	$2^2\cdot3\cdot149$	6	2063*	$2\cdot1031$	5
1801	$2^3\cdot3^2\cdot5^2$	11	2069*	$2^2\cdot11\cdot47$	2
1811*	$2\cdot5\cdot181$	6	2081	$2^5\cdot5\cdot13$	3
1823*	$2\cdot911$	5	2083	$2\cdot3\cdot347$	2
1831	$2\cdot3\cdot5\cdot61$	3	2087	$2\cdot7\cdot149$	5
1847*	$2\cdot13\cdot71$	5	2089	$2^3\cdot3^2\cdot29$	7
1861*	$2^2\cdot3\cdot5\cdot31$	2	2099*	$2\cdot1049$	2
1867	$2\cdot3\cdot311$	2	2111	$2\cdot5\cdot211$	7
1871	$2\cdot5\cdot11\cdot17$	14	2113*	$2^6\cdot3\cdot11$	5
1873*	$2^4\cdot3^2\cdot13$	10	2129	$2^4\cdot7\cdot19$	3
1877	$2^2\cdot7\cdot67$	2	2131	$2\cdot3\cdot5\cdot71$	2
1879	$2\cdot3\cdot313$	6	2137*	$2^3\cdot3\cdot89$	10
1889	$2^5\cdot59$	3	2141*	$2^2\cdot5\cdot107$	2

p	$p-1$	g	p	$p-1$	g
2143*	$2\cdot3^2\cdot7\cdot17$	3	2399	$2\cdot11\cdot109$	11
2153*	$2^3\cdot269$	3	2411*	$2\cdot5\cdot241$	6
2161	$2^4\cdot3^3\cdot5$	23	2417*	$2^4\cdot151$	3
2179*	$2\cdot3^2\cdot11^2$	7	2423*	$2\cdot7\cdot173$	5
2203	$2\cdot3\cdot367$	5	2437*	$2^2\cdot3\cdot7\cdot29$	2
2207*	$2\cdot1103$	5	2441	$2^3\cdot5\cdot61$	6
2213	$2^2\cdot7\cdot79$	2	2447*	$2\cdot1223$	5
2221*	$2^2\cdot3\cdot5\cdot37$	2	2459*	$2\cdot1229$	2
2237	$2^2\cdot13\cdot43$	2	2467	$2\cdot3^2\cdot137$	2
2239	$2\cdot3\cdot373$	3	2473*	$2^3\cdot3\cdot103$	5
2243	$2\cdot19\cdot59$	2	2477	$2^2\cdot619$	2
2251*	$2\cdot3^2\cdot5^3$	7	2503	$2\cdot3^2\cdot139$	3
2267	$2\cdot11\cdot103$	2	2521	$2^3\cdot3^2\cdot5\cdot7$	17
2269*	$2^2\cdot3^4\cdot7$	2	2531	$2\cdot5\cdot11\cdot23$	2
2273*	$2^5\cdot71$	3	2539*	$2\cdot3^3\cdot47$	2
2281	$2^3\cdot3\cdot5\cdot19$	7	2543*	$2\cdot31\cdot41$	5
2287	$2\cdot3^2\cdot127$	19	2549*	$4\cdot7^2\cdot13$	2
2293	$2^2\cdot3\cdot191$	2	2551	$2\cdot3\cdot5^3\cdot17$	6
2297*	$2^3\cdot7\cdot41$	5	2557	$2^2\cdot3^2\cdot71$	2
2309*	$2^2\cdot577$	2	2579*	$2\cdot1289$	2
2311	$2\cdot3\cdot5\cdot7\cdot11$	3	2591	$2\cdot5\cdot7\cdot37$	7
2333	$2^2\cdot11\cdot53$	2	2593*	$2^4\cdot3^4$	7
2339*	$2\cdot7\cdot167$	2	2609	$2^4\cdot163$	3
2341*	$2^2\cdot3^2\cdot5\cdot13$	7	2617*	$2^3\cdot3\cdot109$	5
2347	$2\cdot3\cdot17\cdot23$	3	2621*	$2^2\cdot5\cdot131$	2
2351	$2\cdot5^2\cdot47$	13	2633*	$2^3\cdot7\cdot47$	3
2357	$2^2\cdot19\cdot31$	2	2647	$2\cdot3^3\cdot7^2$	3
2371*	$2\cdot3\cdot5\cdot79$	2	2657*	$2^5\cdot83$	3
2377	$2^3\cdot3^3\cdot11$	5	2659	$2\cdot3\cdot443$	2
2381	$2^2\cdot5\cdot7\cdot17$	3	2663*	$2\cdot11^3$	5
2383*	$2\cdot3\cdot397$	5	2671	$2\cdot3\cdot5\cdot89$	7
2389*	$2^2\cdot3\cdot199$	2	2677	$2^2\cdot3\cdot223$	2
2393	$2^3\cdot13\cdot23$	3	2683	$2\cdot3^2\cdot149$	2

续

p	p-1	g	p	p-1	g
2687*	$2\cdot17\cdot79$	5	2927*	$2\cdot7\cdot11\cdot19$	5
2689	$2^7\cdot3\cdot7$	19	2939*	$2\cdot13\cdot113$	2
2693	$2^2\cdot673$	2	2953	$2^3\cdot3^2\cdot41$	13
2699*	$2\cdot19\cdot71$	2	2957	$2^2\cdot739$	2
2707	$2\cdot3\cdot11\cdot41$	2	2963	$2\cdot1481$	2
2711	$2\cdot5\cdot271$	7	2969	$2^3\cdot7\cdot53$	3
2713*	$2^3\cdot3\cdot113$	5	2971*	$2\cdot3^3\cdot5\cdot11$	10
2719	$2\cdot3^2\cdot151$	3	2999	$2\cdot1499$	17
2729*	$2^3\cdot11\cdot31$	3	3001	$2^3\cdot3\cdot5^3$	14
2731	$2\cdot3\cdot5\cdot7\cdot13$	3	3011*	$2\cdot5\cdot7\cdot43$	2
2741*	$2^2\cdot5\cdot137$	2	3019*	$2\cdot3\cdot503$	2
2749	$2^2\cdot3\cdot229$	6	3023*	$2\cdot1511$	5
2753*	$2^6\cdot43$	3	3037	$2^2\cdot3\cdot11\cdot23$	2
2767*	$2\cdot3\cdot461$	3	3041	$2^5\cdot5\cdot19$	3
2777*	$2^3\cdot347$	3	3049	$2^3\cdot3\cdot127$	11
2789*	$2^2\cdot17\cdot41$	2	3061	$2^2\cdot3^2\cdot5\cdot17$	6
2791	$2\cdot3^2\cdot5\cdot31$	6	3067	$2\cdot3\cdot7\cdot73$	2
2797	$2^2\cdot3\cdot233$	2	3079	$2\cdot3^4\cdot19$	6
2801	$2^4\cdot5^2\cdot7$	3	3083	$2\cdot23\cdot67$	2
2803	$2\cdot3\cdot467$	2	3089	$2^4\cdot193$	3
2819*	$2\cdot1409$	2	3109	$2^2\cdot3\cdot7\cdot37$	6
2833*	$2^4\cdot3\cdot59$	5	3119	$2\cdot1559$	7
2837	$2^2\cdot709$	2	3121	$2^4\cdot3\cdot5\cdot13$	7
2843	$2\cdot7^2\cdot29$	2	3137*	$2^6\cdot7^2$	3
2851*	$2\cdot3\cdot5^2\cdot19$	2	3163	$2\cdot3\cdot17\cdot31$	3
2857	$2^3\cdot3\cdot7\cdot17$	11	3167*	$2\cdot1583$	5
2861*	$2^2\cdot5\cdot11\cdot13$	2	3169	$2^5\cdot3^2\cdot11$	7
2879	$2\cdot1439$	7	3181	$2^2\cdot3\cdot5\cdot53$	7
2887	$2\cdot3\cdot13\cdot37$	5	3187	$2\cdot3^3\cdot59$	2
2897*	$2^4\cdot181$	3	3191	$2\cdot5\cdot11\cdot29$	11
2903*	$2\cdot1451$	5	3203	$2\cdot1601$	2
2909*	$2^2\cdot727$	2	3209	$2^3\cdot401$	3
2917	$2^2\cdot3^6$	5	3217	$2^4\cdot3\cdot67$	5

p	$p-1$	g	p	$p-1$	g
3221*	$2^2\cdot5\cdot7\cdot23$	10	3499	$2\cdot3\cdot11\cdot53$	2
3229	$2^2\cdot3\cdot269$	6	3511	$2\cdot3^3\cdot5\cdot13$	7
3251*	$2\cdot5^3\cdot13$	6	3517	$2^2\cdot3\cdot293$	2
3253	$2^2\cdot3\cdot271$	2	3527*	$2\cdot41\cdot43$	5
3257*	$2^3\cdot11\cdot37$	3	3529	$2^3\cdot3^2\cdot7^2$	17
3259*	$2\cdot3^2\cdot181$	3	3533	$2^2\cdot883$	2
3271	$2\cdot3\cdot5\cdot109$	3	3539*	$2\cdot29\cdot61$	2
3299*	$2\cdot17\cdot97$	2	3541	$2^2\cdot3\cdot5\cdot59$	7
3301*	$2^2\cdot3\cdot5^2\cdot11$	6	3547	$2\cdot3^2\cdot197$	2
3307	$2\cdot3\cdot19\cdot29$	2	3557	$2^2\cdot7\cdot127$	2
3313*	$2^4\cdot3^2\cdot23$	10	3559	$2\cdot3\cdot593$	3
3319	$2\cdot3\cdot7\cdot79$	6	3571*	$2\cdot3\cdot5\cdot7\cdot17$	2
3323	$2\cdot11\cdot151$	2	3581*	$2^2\cdot5\cdot179$	2
3329	$2^8\cdot13$	3	3583	$2\cdot3^2\cdot199$	3
3331*	$2\cdot3^2\cdot5\cdot37$	3	3593*	$2^3\cdot449$	3
3343*	$2\cdot3\cdot557$	5	3607*	$2\cdot3\cdot601$	5
3347	$2\cdot7\cdot239$	2	3613	$2^2\cdot3\cdot7\cdot43$	2
3359	$2\cdot23\cdot73$	11	3617*	$2^5\cdot113$	3
3361	$2^5\cdot3\cdot5\cdot7$	22	3623*	$2\cdot1811$	5
3371*	$2\cdot5\cdot337$	2	3631	$2\cdot3\cdot5\cdot11^2$	15
3373	$2^2\cdot3\cdot281$	5	3637	$2^2\cdot3^2\cdot101$	2
3389*	$2^2\cdot7\cdot11^2$	3	3643	$2\cdot3\cdot607$	2
3391	$2\cdot3\cdot5\cdot113$	3	3659*	$2\cdot31\cdot59$	2
3407*	$2\cdot13\cdot131$	5	3671	$2\cdot5\cdot367$	13
3413	$2^2\cdot853$	2	3673*	$2^3\cdot3^3\cdot17$	5
3433*	$2^3\cdot3\cdot11\cdot13$	5	3677	$2^2\cdot919$	2
3449	$2^3\cdot431$	3	3691	$2\cdot3^2\cdot5\cdot41$	2
3457	$2^7\cdot3^3$	7	3697	$2^4\cdot3\cdot7\cdot11$	5
3461*	$2^2\cdot5\cdot173$	2	3701*	$2^2\cdot5^2\cdot37$	2
3463*	$2\cdot3\cdot577$	3	3709*	$2^2\cdot3^2\cdot103$	2
3467	$2\cdot1733$	2	3719	$2\cdot11\cdot13^2$	7
3469*	$2^2\cdot3\cdot17^2$	2	3727*	$2\cdot3^4\cdot23$	3
3491	$2\cdot5\cdot349$	2	3733	$2^2\cdot3\cdot311$	2

p	$p-1$	g	p	$p-1$	g
3739	$2\cdot3\cdot7\cdot89$	7	4019*	$2\cdot7^2\cdot41$	2
3761	$2^4\cdot5\cdot47$	3	4021	$2^2\cdot3\cdot5\cdot67$	2
3767	$2\cdot7\cdot269$	5	4027	$2\cdot3\cdot11\cdot61$	3
3769	$2^3\cdot3\cdot157$	7	4049	$2^4\cdot11\cdot23$	3
3779*	$2\cdot1889$	2	4051*	$2\cdot3^4\cdot5^2$	10
3793	$2^4\cdot3\cdot79$	5	4057*	$2^3\cdot3\cdot13^2$	5
3797	$2^2\cdot13\cdot73$	2	4073*	$2^3\cdot509$	3
3803	$2\cdot1901$	2	4079	$2\cdot2039$	11
3821*	$2^2\cdot5\cdot191$	3	4091*	$2\cdot5\cdot409$	2
3823	$2\cdot3\cdot7^2\cdot13$	3	4093	$2^2\cdot3\cdot11\cdot31$	2
3833*	$2^3\cdot479$	3	4099	$2\cdot3\cdot683$	2
3847*	$2\cdot3\cdot641$	5	4111	$2\cdot3\cdot5\cdot137$	12
3851*	$2\cdot5^2\cdot7\cdot11$	2	4127	$2\cdot2063$	5
3853	$2^2\cdot3^2\cdot107$	2	4129	$2^5\cdot3\cdot43$	13
3863*	$2\cdot1931$	5	4133	$2^2\cdot1033$	2
3877	$2^2\cdot3\cdot17\cdot19$	2	4139*	$2\cdot2069$	2
3881	$2^3\cdot5\cdot97$	13	4153*	$2^3\cdot3\cdot173$	5
3889	$2^4\cdot3^5$	11	4157	$2^2\cdot1039$	2
3907	$2\cdot3^2\cdot7\cdot31$	2	4159	$2\cdot3^3\cdot7\cdot11$	3
3911	$2\cdot5\cdot17\cdot23$	13	4177*	$2^4\cdot3^2\cdot29$	5
3917	$2^2\cdot11\cdot89$	2	4201	$2^3\cdot3\cdot5^2\cdot7$	11
3919	$2\cdot3\cdot653$	3	4211*	$2\cdot5\cdot421$	6
3923	$2\cdot37\cdot53$	2	4217*	$2^3\cdot17\cdot31$	3
3929	$2^3\cdot491$	3	4219*	$2\cdot3\cdot19\cdot37$	2
3931	$2\cdot3\cdot5\cdot131$	2	4229*	$2^2\cdot7\cdot151$	2
3943*	$2\cdot3^3\cdot73$	3	4231	$2\cdot3^2\cdot5\cdot47$	3
3947	$2\cdot1973$	2	4241	$2^4\cdot5\cdot53$	3
3967*	$2\cdot3\cdot661$	6	4243	$2\cdot3\cdot7\cdot101$	2
3989*	$2^2\cdot997$	2	4253	$2^2\cdot1063$	2
4001	$2^5\cdot5^3$	3	4259*	$2\cdot2129$	2
4003	$2\cdot3\cdot23\cdot29$	2	4261*	$2^2\cdot3\cdot5\cdot71$	2
4007*	$2\cdot2003$	5	4271	$2\cdot5\cdot7\cdot61$	7
4013	$2^2\cdot17\cdot59$	2	4273	$2^4\cdot3\cdot89$	5

续

p	$p-1$	g	p	$p-1$	g
4283	$2\cdot2141$	2	4591	$2\cdot3^3\cdot5\cdot17$	11
4289	$2^6\cdot67$	3	4597	$2^2\cdot3\cdot383$	5
4297	$2^3\cdot3\cdot179$	5	4603	$2\cdot3\cdot13\cdot59$	2
4327*	$2\cdot3\cdot7\cdot103$	3	4621	$2^2\cdot3\cdot5\cdot7\cdot11$	2
4337*	$2^4\cdot271$	3	4637	$2^2\cdot19\cdot61$	2
4339*	$2\cdot3^2\cdot241$	10	4639	$2\cdot3\cdot773$	3
4349*	$2^2\cdot1087$	2	4643	$2\cdot11\cdot211$	5
4357	$2^2\cdot3^2\cdot11^2$	2	4649	$2^3\cdot7\cdot83$	3
4363	$2\cdot3\cdot727$	2	4651*	$2\cdot3\cdot5^2\cdot31$	3
4373	$2^2\cdot1093$	2	4657	$2^4\cdot3\cdot97$	15
4391	$2\cdot5\cdot439$	14	4663	$2\cdot3^2\cdot7\cdot37$	3
4397	$2^2\cdot7\cdot157$	2	4673*	$2^6\cdot73$	3
4409	$2^3\cdot19\cdot29$	3	4679	$2\cdot2339$	11
4421*	$2^2\cdot5\cdot13\cdot17$	3	4691*	$2\cdot5\cdot7\cdot67$	2
4423*	$2\cdot3\cdot11\cdot67$	3	4703*	$2\cdot2351$	5
4441	$2^3\cdot3\cdot5\cdot37$	21	4721	$2^4\cdot5\cdot59$	6
4447*	$2\cdot3^2\cdot13\cdot19$	3	4723	$2\cdot3\cdot787$	2
4451*	$2\cdot5^2\cdot89$	2	4729	$2^3\cdot3\cdot197$	17
4457*	$2^3\cdot557$	3	4733	$2^2\cdot7\cdot13^2$	5
4463*	$2\cdot23\cdot97$	5	4751	$2\cdot5^3\cdot19$	19
4481	$2^7\cdot5\cdot7$	3	4759	$2\cdot3\cdot13\cdot61$	3
4483	$2\cdot3^3\cdot83$	2	4783*	$2\cdot3\cdot797$	6
4493	$2^2\cdot1123$	2	4787	$2\cdot2393$	2
4507	$2\cdot3\cdot751$	2	4789	$2^2\cdot3^2\cdot7\cdot19$	2
4513	$2^5\cdot3\cdot47$	7	4793*	$2^3\cdot599$	3
4517	$2^2\cdot1129$	2	4799	$2\cdot2399$	7
4519	$2\cdot3^2\cdot251$	3	4801	$2^6\cdot3\cdot5^2$	7
4523	$2\cdot7\cdot17\cdot19$	5	4813	$2^2\cdot3\cdot401$	2
4547	$2\cdot2273$	2	4817*	$2^4\cdot7\cdot43$	3
4549	$2^2\cdot3\cdot379$	6	4831	$2\cdot3\cdot5\cdot7\cdot23$	3
4561	$2^4\cdot3\cdot5\cdot19$	11	4861	$2^2\cdot3^5\cdot5$	11
4567*	$2\cdot3\cdot761$	3	4871	$2\cdot5\cdot487$	11
4583*	$2\cdot29\cdot79$	5	4877	$2^2\cdot23\cdot53$	2

p	$p-1$	g	p	$p-1$	g
4889	$2^3\cdot13\cdot47$	3	4951	$2\cdot3^2\cdot5^2\cdot11$	6
4903	$2\cdot3\cdot19\cdot43$	3	4957	$2^2\cdot3\cdot7\cdot59$	2
4909	$2^2\cdot3\cdot409$	6	4967*	$2\cdot13\cdot191$	5
4919	$2\cdot2459$	13	4969	$2^3\cdot3^3\cdot23$	11
4931*	$2\cdot5\cdot17\cdot29$	6	4973	$2^2\cdot11\cdot113$	2
4933	$2^2\cdot3^2\cdot137$	2	4987	$2\cdot3^2\cdot277$	2
4937*	$2^3\cdot617$	3	4993	$2^7\cdot3\cdot13$	5
4943*	$2\cdot7\cdot353$	7	4999	$2\cdot3\cdot7^2\cdot17$	3

附表2　$\sqrt{d}$ 的连分数与 Pell 方程的最小正解表($2\leqslant d\leqslant 100$)

($x_0+y_0\sqrt{d}$ (+1或−1)分别表示$x^2-dy^2=+1$或−1的最小正解)

d	$\sqrt{d}$ 的连分数	$x_0+y_0\sqrt{d}$	d	$\sqrt{d}$ 的连分数	$x_0+y_0\sqrt{d}$
2	$\langle 1,\overline{2}\rangle$	$1+\sqrt{2}$　(−1)	19	$\langle 4,\overline{2,1,3,1,2,8}\rangle$	$170+39\sqrt{19}$　(+1)
3	$\langle 1,\overline{1,2}\rangle$	$2+\sqrt{3}$　(+1)	20	$\langle 4,\overline{2,8}\rangle$	$9+2\sqrt{20}$　(+1)
5	$\langle 2,\overline{4}\rangle$	$2+\sqrt{5}$　(−1)	21	$\langle 4,\overline{1,1,2,1,1,8}\rangle$	$55+12\sqrt{21}$　(+1)
6	$\langle 2,\overline{2,4}\rangle$	$5+2\sqrt{6}$　(+1)	22	$\langle 4,\overline{1,2,4,2,1,8}\rangle$	$197+42\sqrt{22}$　(+1)
7	$\langle 2,\overline{1,1,1,4}\rangle$	$8+3\sqrt{7}$　(+1)	23	$\langle 4,\overline{1,3,1,8}\rangle$	$24+5\sqrt{23}$　(+1)
8	$\langle 2,\overline{1,4}\rangle$	$3+\sqrt{8}$　(+1)	24	$\langle 4,\overline{1,8}\rangle$	$5+\sqrt{24}$　(+1)
10	$\langle 3,\overline{6}\rangle$	$3+\sqrt{10}$　(−1)	26	$\langle 5,\overline{10}\rangle$	$5+\sqrt{26}$　(−1)
11	$\langle 3,\overline{3,6}\rangle$	$10+3\sqrt{11}$　(+1)	27	$\langle 5,\overline{5,10}\rangle$	$26+5\sqrt{27}$　(+1)
12	$\langle 3,\overline{2,6}\rangle$	$7+2\sqrt{12}$　(+1)	28	$\langle 5,\overline{3,2,3,10}\rangle$	$127+24\sqrt{28}$　(+1)
13	$\langle 3,\overline{1,1,1,1,6}\rangle$	$18+5\sqrt{13}$　(−1)	29	$\langle 5,\overline{2,1,1,2,10}\rangle$	$70+13\sqrt{29}$　(−1)
14	$\langle 3,\overline{1,2,1,6}\rangle$	$15+4\sqrt{14}$　(+1)	30	$\langle 5,\overline{2,10}\rangle$	$11+2\sqrt{30}$　(+1)
15	$\langle 3,\overline{1,6}\rangle$	$4+\sqrt{15}$　(+1)	31	$\langle 5,\overline{1,1,3,5,3,1,1,10}\rangle$	$1520+273\sqrt{31}$　(+1)
17	$\langle 4,\overline{8}\rangle$	$4+\sqrt{17}$　(−1)	32	$\langle 5,\overline{1,1,1,10}\rangle$	$17+3\sqrt{32}$　(+1)
18	$\langle 4,\overline{4,8}\rangle$	$17+4\sqrt{18}$　(+1)	33	$\langle 5,\overline{1,2,1,10}\rangle$	$23+4\sqrt{33}$　(+1)

续

d	$\sqrt{d}$ 的连分数	$x_0+y_0\sqrt{d}$		d	$\sqrt{d}$ 的连分数	$x_0+y_0\sqrt{d}$	
34	$\langle 5,\overline{1,4,1,10}\rangle$	$35+6\sqrt{34}$	$(+1)$	52	$\langle 7,\overline{4,1,2,1,4,14}\rangle$	$649+90\sqrt{52}$	$(+1)$
35	$\langle 5,\overline{1,10}\rangle$	$6+\sqrt{35}$	$(+1)$	53	$\langle 7,\overline{3,1,1,3,14}\rangle$	$182+25\sqrt{53}$	(-1)
37	$\langle 6,\overline{12}\rangle$	$6+\sqrt{37}$	(-1)	54	$\langle 7,\overline{2,1,6,1,2,14}\rangle$	$485+66\sqrt{54}$	$(+1)$
38	$\langle 6,\overline{6,12}\rangle$	$37+6\sqrt{38}$	$(+1)$	55	$\langle 7,\overline{2,2,2,14}\rangle$	$89+12\sqrt{55}$	$(+1)$
39	$\langle 6,\overline{4,12}\rangle$	$25+4\sqrt{39}$	$(+1)$	56	$\langle 7,\overline{2,14}\rangle$	$15+2\sqrt{56}$	$(+1)$
40	$\langle 6,\overline{3,12}\rangle$	$19+3\sqrt{40}$	$(+1)$	57	$\langle 7,\overline{1,1,4,1,1,14}\rangle$	$151+20\sqrt{57}$	$(+1)$
41	$\langle 6,\overline{2,2,12}\rangle$	$32+5\sqrt{41}$	(-1)	58	$\langle 7,\overline{1,1,1,1,1,1,14}\rangle$	$99+13\sqrt{58}$	$(+1)$
42	$\langle 6,\overline{2,12}\rangle$	$13+2\sqrt{42}$	$(+1)$	59	$\langle 7,\overline{1,2,7,2,1,14}\rangle$	$530+69\sqrt{59}$	$(+1)$
43	$\langle 6,\overline{1,1,3,1,5,1,3,1,1,12}\rangle$	$3482+531\sqrt{43}$	$(+1)$	60	$\langle 7,\overline{1,2,1,14}\rangle$	$31+4\sqrt{60}$	$(+1)$
44	$\langle 6,\overline{1,1,1,2,1,1,1,12}\rangle$	$199+30\sqrt{44}$	$(+1)$	61	$\langle 7,\overline{1,4,3,1,2,2,1,3,4,1,14}\rangle$	$29718+3805\sqrt{61}$	(-1)
45	$\langle 6,\overline{1,2,2,2,1,12}\rangle$	$161+24\sqrt{45}$	$(+1)$	62	$\langle 7,\overline{1,6,1,14}\rangle$	$63+8\sqrt{62}$	$(+1)$
46	$\langle 6,\overline{1,3,1,1,2,6,2,1,1,3,1,12}\rangle$	$24335+3588\sqrt{46}$	$(+1)$	63	$\langle 7,\overline{1,14}\rangle$	$8+\sqrt{64}$	$(+1)$
				65	$\langle 8,\overline{16}\rangle$	$8+\sqrt{65}$	(-1)
47	$\langle 6,\overline{1,5,1,12}\rangle$	$48+7\sqrt{47}$	$(+1)$	66	$\langle 8,\overline{8,16}\rangle$	$65+8\sqrt{66}$	$(+1)$
48	$\langle 6,\overline{1,12}\rangle$	$7+\sqrt{48}$	$(+1)$	67	$\langle 8,\overline{5,2,1,1,7,1,1,2,5,16}\rangle$	$48842+5967\sqrt{67}$	$(+1)$
50	$\langle 7,\overline{14}\rangle$	$7+\sqrt{50}$	(-1)	68	$\langle 8,\overline{4,16}\rangle$	$33+4\sqrt{68}$	$(+1)$
51	$\langle 7,\overline{7,14}\rangle$	$50+7\sqrt{51}$	$(+1)$	69	$\langle 8,\overline{3,3,1,4,1,3,3,16}\rangle$	$7775+936\sqrt{69}$	$(+1)$

续

d	$\sqrt{d}$的连分数	$x_0+y_0\sqrt{d}$		d	$\sqrt{d}$的连分数	$x_0+y_0\sqrt{d}$	
70	$\langle 8,\overline{2,1,2,1,2,16}\rangle$	$251+30\sqrt{70}$	(+1)	86	$\langle 9,\overline{3,1,1,1,8,1,1,1,3,18}\rangle$	$10405+1122\sqrt{86}$	(+1)
71	$\langle 8,\overline{2,2,1,7,1,2,2,16}\rangle$	$3480+413\sqrt{71}$	(+1)	87	$\langle 9,\overline{3,18}\rangle$	$28+3\sqrt{87}$	(+1)
72	$\langle 8,\overline{2,16}\rangle$	$17+2\sqrt{72}$	(+1)	88	$\langle 9,\overline{2,1,1,1,2,18}\rangle$	$197+21\sqrt{88}$	(+1)
73	$\langle 8,\overline{1,1,5,5,1,1,16}\rangle$	$1068+125\sqrt{73}$	(−1)	89	$\langle 9,\overline{2,3,3,2,18}\rangle$	$500+53\sqrt{89}$	(−1)
74	$\langle 8,\overline{1,1,1,1,16}\rangle$	$43+5\sqrt{74}$	(−1)	90	$\langle 9,\overline{2,18}\rangle$	$19+2\sqrt{90}$	(+1)
75	$\langle 8,\overline{1,1,1,16}\rangle$	$26+3\sqrt{75}$	(+1)	91	$\langle 9,\overline{1,1,5,1,5,1,1,18}\rangle$	$1574+165\sqrt{91}$	(+1)
76	$\langle 8,\overline{1,2,1,1,5,4,5,1,1,2,1,16}\rangle$	$57799+6630\sqrt{76}$	(+1)	92	$\langle 9,\overline{1,1,2,4,2,1,1,18}\rangle$	$1151+120\sqrt{92}$	(+1)
77	$\langle 8,\overline{1,3,2,3,1,16}\rangle$	$351+40\sqrt{77}$	(+1)	93	$\langle 9,\overline{1,1,1,4,6,4,1,1,1,18}\rangle$	$12151+1260\sqrt{93}$	(+1)
78	$\langle 8,\overline{1,4,1,16}\rangle$	$53+6\sqrt{78}$	(+1)	94	$\langle 9,\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}\rangle$	$2143295+221064\sqrt{94}$	(+1)
79	$\langle 8,\overline{1,7,1,16}\rangle$	$80+9\sqrt{79}$	(+1)	95	$\langle 9,\overline{1,2,1,18}\rangle$	$39+4\sqrt{95}$	(+1)
80	$\langle 8,\overline{1,16}\rangle$	$9+\sqrt{80}$	(+1)	96	$\langle 9,\overline{1,3,1,18}\rangle$	$49+5\sqrt{96}$	(+1)
82	$\langle 9,\overline{18}\rangle$	$9+\sqrt{82}$	(−1)	97	$\langle 9,\overline{1,5,1,1,1,1,1,1,5,1,18}\rangle$	$5604+569\sqrt{97}$	(−1)
83	$\langle 9,\overline{9,18}\rangle$	$82+9\sqrt{83}$	(+1)	98	$\langle 9,\overline{1,8,1,18}\rangle$	$99+10\sqrt{98}$	(+1)
84	$\langle 9,\overline{6,18}\rangle$	$55+6\sqrt{84}$	(+1)	99	$\langle 9,\overline{1,18}\rangle$	$10+\sqrt{99}$	(+1)
85	$\langle 9,\overline{4,1,1,4,18}\rangle$	$378+41\sqrt{85}$	(−1)				

参 考 书 目①

[1] U. Dudley, Elementary Number Theory, 2nd ed., W. H. Freeman and Company, 1978.(周仲良译，基础数论，上海科学技术出版社，1980.)

[2] 华罗庚，数论导引，科学出版社，1957.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford, 1981.

[4] 柯召、孙琦，谈谈不定方程，上海教育出版社，1980.

[5] 闵嗣鹤、严士健，初等数论，人民教育出版社，1957.

[6] T. Nagell, Introduction to Number Theory, Wiley, 1951.

[7] I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 4th ed., Wiley, 1980.

[8] O. Ore, An Invitation to Number Theory, Random House, 1967.(潘承彪译，有趣的数论，北京大学出版社，1985.)

[9] H. E. Rose, A Course in Number Theory, Oxford, 1988.

[10] K. H. Rosen, Elementary Number Theory and Its Applications, Addison-Wesley, 1984.

[11] W. Sierpiński, Elementary Theory of Numbers, PAN, 1964.

[12] И. М. Виноградов, Основы Теории Чисел, Изд. Дев., Hayka, 1981 (第五版，裘光明译，数论基础，商务印书馆，1952).

---

① 这里列出的是我们在写本书时参考较多的初等数论书。还应该推荐 R. P. Burn 的 A Pathway into Number Theory, Cambridge, 1982 (于秀源译，数论入门，高等教育出版社，1990)，这是一本以习题形式出现的非常适合于自学的好教材。